21世纪高等学校规划教材 | 计算机科学与技术



网络安全技术与应用实践

刘远生 主编
辛一 李民 副主编

清华大学出版社

21 世纪高等学校规划教材·计算机科学与技术

网络安全技术与应用实践

刘远生　主　编
辛　一　李　民　副主编

清 华 大 学 出 版 社
北　京

内 容 简 介

本书从网络系统安全管理和应用的角度出发，重点介绍网络安全技术及其应用，各章在介绍网络安全技术后均配以相应的实践内容或应用实例，体现培养读者网络安全及管理技术的应用能力和实践操作技能的特色。

本书对原理、技术难点的介绍适度，将理论知识和实际应用紧密地结合在一起，典型实例的应用性和可操作性强；章末配有习题和思考题，便于学生学习和实践，内容安排合理，重点突出，文字简明，语言通俗易懂。

本书可作为普通高校计算机、通信、信息安全等专业的应用型本科、高职高专或成人教育学生的网络安全实践教材，也可作为网络管理人员、网络工程技术人员和信息安全管理人员及对网络安全感兴趣读者的参考书。

图书在版编目（CIP）数据

网络安全技术与应用实践/刘远生主编. —北京：清华大学出版社，2010.8
（21世纪高等学校规划教材·计算机科学与技术）
ISBN 978-7-302-22619-2

Ⅰ. ①网…　Ⅱ. ①刘…　Ⅲ. ①计算机网络－安全技术－高等学校－教材
Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2010)第081858号

责任编辑：付弘宇　李玮琪
责任校对：白　蕾
责任印制：

出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：185×260　　**印　张**：20.5　　**字　数**：498千字
版　次：2010年8月第1版　　**印　次**：2010年8月第1次印刷
印　数：1～　000
定　价：　.00元

产品编号：

编审委员会成员

（按地区排序）

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程(简称‘质量工程’)”，通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程(群)加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”(以下简称“编委会”)，旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性(新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量)、先进性(对原有的学科体系有实质性的改革和发展，顺应并符合 21 世纪教学发展的规律，代表并引领课程发展的趋势和方向)、示范性(教材所体现的课程体系具有较广泛的辐射性和示范性)和一定的前瞻性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐)，经“编委会”认真评审，最后由清华大学出版

社审定出版。

目前，针对计算机类和电子信息类相关专业成立了两个“编委会”，即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括：

（1）21世纪高等学校规划教材·计算机应用——高等学校各类专业，特别是非计算机专业的计算机应用类教材。

（2）21世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

（3）21世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

（4）21世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

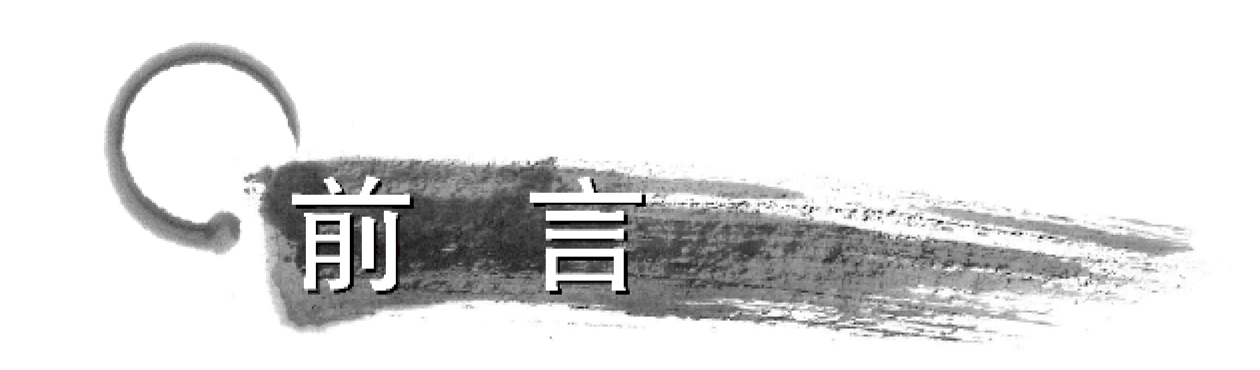
（5）21世纪高等学校规划教材·信息管理与信息系统。

（6）21世纪高等学校规划教材·财经管理与计算机应用。

（7）21世纪高等学校规划教材·电子商务。

清华大学出版社经过二十多年的努力，在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌，为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格，这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会
联系人：魏江江
E-mail：weijj@tup.tsinghua.edu.cn



前 言

随着 Internet 的发展和计算机网络的普及应用，人们的学习、工作和生活方式有了极大的改变。在计算机网络为人们带来方便的同时，网络系统的安全问题也变得日益突出和复杂。解决网络安全问题更多地涉及网络安全技术、网络系统管理和实际应用。每一位相关专业的学生、网络机构的管理人员、工程技术人员，乃至普通网络用户都应该掌握一定的计算机网络安全知识和技术，以使自己的信息系统能够安全、稳定地运行，并提供正常的服务。当然，解决网络系统的安全问题是一个系统工程，它不仅涉及技术问题，还涉及管理、法律和道德，是一个社会问题。

目前关于网络安全的教材和参考书已很多，但一般都是理论知识和技术原理介绍得较多较深，网络安全的实际案例、软件工具应用和实际操作技能介绍得较少，比较适合于研究型大学的本科生或研究生使用。而对于应用型本科和高职、大专学生而言，在了解简单的网络安全知识和技术原理的基础上，应重点掌握和熟练运用相关的网络安全技术和实际解决方案。

本书在介绍网络安全基本知识的基础上，重点介绍了网络安全技术及其应用。在内容上除第 1 章简单介绍有关网络安全的概念、安全策略和安全管理知识外，此后各章在介绍的相关网络安全技术后均配以相应的实践内容或应用实例，旨在培养学生的实际动手能力和解决问题的操作技能。

本书从网络系统安全管理和应用的角度出发，强调理论联系实际，体现培养学生的网络管理、安全技术应用能力和实践操作技能的特色。全书共有 9 章，内容包括网络安全概述、网络设备的安全与应用实践、网络操作系统安全与管理实践、数据加密技术与应用实践、软件安全技术与应用实践、网络攻防技术与应用实践、VPN 安全技术与应用实践、无线网络的安全与应用实践和电子邮件安全与应用实践等。

本书对网络安全的理论和技术原理等介绍适度，典型实例的应用性和可操作性强，章末配有习题和思考题，便于学生学习和实践。本书可作为普通高校计算机专业、通信专业及相关专业的本科生、大专生教材，也可作为网络管理人员、网络工程技术人员和信息安全管理人员以及对网络安全感兴趣读者的参考书。

本书由刘远生任主编，辛一、李民任副主编，参加编写的还有薛庆水、张明辉、丛晓红、刘芊麟、刘野等，全书由刘远生统阅定稿。在本书的编写过程中得到了清华大学出版社编辑的大力支持和帮助，在此表示衷心的感谢。

由于编者水平有限，书中难免存在缺点和不足之处，殷切希望各位读者提出宝贵意见，恳请各位专家、学者给予批评指正。编者也希望与各位读者多多交流，联系邮箱为 ysliu@sjtu.edu.cn。

本书的配套课件等资料可以从清华大学出版社网站(http://www.tup.tsinghua.edu.cn)下载，相关问题联系 fuhy@tup.tsinghua.edu.cn。

编者

2010 年 4 月

于上海交通大学

目 录

第1章 网络安全概述

计算机网络技术是由现代通信技术和计算机技术的高速发展、密切结合而产生和发展起来的，是20世纪最伟大的科学技术成就之一。计算机网络的发展速度又超过了世界上任何一种其他科学技术的发展速度。计算机技术与通信技术的结合使计算机的应用范围得到了极大的开拓。

计算机网络的发展，特别是Internet的发展和普及应用，为人类带来了新的工作、学习和生活方式，计算机网络和人们的工作与生活的联系也越来越密切。计算机网络系统提供了丰富的资源以便用户共享，提高了系统的灵活性和便捷性。通过网络，人们可以与远在天涯的朋友互发函件，可以足不出户地浏览世界各地的报纸杂志，搜索自己所需的信息，可以在家里与世界各个角落的陌生人打牌下棋……但与此同时，人们也发现自己的计算机信息系统不断受到侵害，其形式多样化，技术先进且复杂化，令人防不胜防。

如何使计算机网络系统不受破坏，提高系统的安全可靠性，已成为人们关注和亟须解决的问题。每个网络机构的管理人员、网络系统用户和工程技术人员都应该掌握一定的计算机网络安全技术，以使自己的信息系统能够安全稳定地运行并提供正常的安全服务。

1.1 网络安全概论

计算机网络系统的安全问题变得日益突出和复杂。一方面，计算机网络系统提供了丰富的资源以便用户共享；另一方面，也增加了网络系统的脆弱性和网络安全的复杂性，资源共享增加了网络受威胁和攻击的可能性。事实上，资源共享和网络安全是一对矛盾，随着资源共享的加强，网络安全的问题也日益突出。因此，为使计算机网络系统不受破坏，提高系统的安全可靠性已成为人们关注和必须解决的问题。每个计算机用户也应该掌握一定的计算机网络安全技术，以使自己的信息系统能够安全、稳定地运行。

1.1.1 网络安全的概念

1. 网络安全的含义

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息论、应用数学、信息安全技术等多种学科的综合性学科。网络安全是指利用各种网络管理、控制和技术措施，使网络系统的硬件、软件及其系统中的数据资源受到保护，不因一些不利因素影响而使这些资源遭到破坏、更改、泄露，保证网络系统连续、可靠、安全地运行。

计算机网络安全归根到底就是：确保计算机网络环境下信息系统的安全运行和在信息系统中存储、处理和传输的信息受到安全保护，这就是通常所说的保证网络系统运行的可靠性，确保信息的保密性、完整性、可用性和真实性。

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、可控性和真实性的相关技术和理论都是网络安全的研究领域。

由于现代的数据处理系统都是建立在计算机网络基础上的，计算机网络安全也就是信息系统安全。网络安全同样也包括系统安全运行和系统信息安全保护两方面，即网络安全是对信息系统的安全运行（系统的可靠性）和运行在信息系统中的信息进行安全保护（包括信息的保密性、完整性和可用性保护）的统称。信息系统的安全运行是信息系统提供有效服务（即可用性）的前提，信息的安全保护主要是确保数据信息的保密性和完整性。

2. 网络安全的特征

由上述可知，网络安全的主要特征就是保证网络安全的主要目标，即保证系统的可靠性、软件及数据的完整性。

（1）网络系统的可靠性（reliability）是系统正常运行的特性，即指保证网络系统不因各种因素的影响而中断正常工作。

（2）信息的完整性（integrity）是信息未经授权不能进行改变的特性。一方面是指在系统中存储和传输的信息不被非法操作，即保证信息不被插入、更改、替换和删除，数据分组不丢失、乱序，数据库或系统中的数据不被破坏；另一方面是指信息处理方法的正确性，因为不当的操作可能使数据文件丢失。

（3）信息的可用性（availability）是可被授权实体访问并按需求使用的特性，即指信息和相关的信息资产在授权人需要时可以立即获得，在保证信息完整性的同时，能使这些信息被正常地利用和操作。

（4）信息的保密性（confidentiality）是信息不泄露给非授权用户、实体或过程的特性。利用密码技术对数据进行加密处理后，即可保证信息仅仅为那些被授权使用的人得到，而不被非授权人识别。

1.1.2 网络安全需求与安全目标

网络安全是一个系统的概念，有效的安全策略的制定是网络信息安全的首要目标。通过对网络结构、网络安全的风险分析，对于不同的安全风险可以采用不同的安全措施加以解决，使网络安全达到一定的安全目标。

1. 安全需求

（1）物理安全需求

针对重要信息可能通过电磁辐射或线路干扰等泄露的问题，需要对存放机密信息的机房进行必要的干扰和屏蔽设计。采用辐射干扰机，防止电磁辐射泄露机密信息；通过对其他重要设备进行备份，对重要系统进行备份等进行安全保护。

(2) 访问控制需求

访问控制包括防范非法用户对网络的非法访问、防范合法用户对网络资源的非授权访问和防范假冒合法用户对网络的非法访问。非法用户对网络的访问多为黑客或间谍的攻击行为；合法用户的非授权访问是指合法用户在没有得到许可的情况下访问了他本不该访问的资源；假冒合法用户对网络的非法访问是指非网络用户假冒网络用户的 IP 地址或用户名等资源对网络进行的访问。

(3) 加密设备需求

加密传输是保护网络信息安全的重要手段之一。信息的泄露很大程度上都是因为在链路上被搭线窃取的，数据也可能因为在链路上被截获、篡改后传输给对方，使其真实性、完整性得不到保证。如果利用加密设备对传输的数据进行加密，使得在网上传输的数据以密文形式出现，则即使这些信息在传输过程中被截获，入侵者也读不懂，而且加密机还能通过先进的技术手段对数据传输过程中的完整性、真实性进行鉴别。可以保证数据的保密性、完整性及可靠性。因此，必须配备加密设备对数据进行传输加密。

(4) 入侵检测系统需求

防火墙是实现网络安全最基本、最经济、最有效的措施之一，它可对通过它的所有访问进行严格控制(允许、禁止、报警)。若以为网络配了防火墙就安全了的想法是错误的。因为网络安全是整体的、动态的，不是单一产品能够完全实现的。防火墙不可能完全防止所有的攻击，特别是新的攻击，也不能阻止那些绕过它的攻击。所以确保网络更加安全必须配备入侵检测系统，应对透过防火墙的攻击进行检测并做相应反应(记录、报警、阻断)。

(5) 安全风险评估系统需求

网络系统存在安全漏洞和操作系统漏洞，这是黑客等入侵者攻击屡屡得手的重要原因。入侵者通常是通过一些程序来探测网络系统中存在的安全漏洞，然后对这些漏洞采取相应的技术进行攻击。因此，必须配备网络安全扫描系统检测网络中存在的安全漏洞，采用相应的措施填补系统漏洞，并对网络设备等存在的不安全配置重新进行安全配置。

(6) 防病毒系统需求

针对网络病毒危害性大且传播迅速的特点，必须配备从单机到服务器的整套防病毒软件，实现全网的病毒安全防护。

2. 安全目标

基于以上的需求分析，网络系统可以实现以下安全目标。

- 保护网络系统中存储和传输信息的保密性和完整性。
- 保护网络系统的可用性。
- 保护网络系统服务的可靠性。
- 保证网络资源访问的可控性(防范非法访问及非授权访问)。
- 防范入侵者的恶意攻击与破坏。
- 防范病毒的侵害。
- 保证网络系统的灾难恢复能力。
- 实现网络的安全管理。

1.2 网络的不安全因素

影响网络系统安全的因素很多，但不外乎来自网络系统外部的威胁、破坏和来自系统内部的缺陷(脆弱性)。下面就网络系统的脆弱性和网络系统受到的主要威胁进行探讨。

1.2.1 网络系统的漏洞

计算机网络本身存在一些固有的弱点(脆弱性)，非授权用户利用这些脆弱性可对网络系统进行非法访问，这种非法访问会使系统内数据的完整性受到威胁，也可能使信息遭到破坏而不能继续使用，更为严重的是有价值的信息被窃取而不留任何痕迹。

网络系统的脆弱性主要表现为以下几方面。

1. 操作系统的脆弱性

网络操作系统体系结构本身就是不安全的，具体表现如下。

(1) 动态连接

为了系统集成和系统扩充的需要，操作系统采用动态连接结构，系统的服务和 I/O 操作都可以补丁方式进行升级和动态连接。这种方式虽然为厂商和用户提供了方便，但同时也为黑客提供了入侵的方便(漏洞)，这种动态连接也是计算机病毒产生的温床。

(2) 创建进程

操作系统可以创建进程，而且这些进程可在远程节点上被创建与激活，更加严重的是被创建的进程又可以继续创建其他进程。这样，若黑客在远程将“间谍”程序以补丁方式附在合法用户，特别是超级用户上，就能摆脱系统进程与作业监视程序的检测。

(3) 空口令和 RPC

操作系统为维护方便而预留的无口令入口和提供的远程过程调用(RPC)服务都是黑客进入系统的通道。

(4) 超级用户

操作系统的另一个安全漏洞就是存在超级用户，如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者。

2. 计算机系统本身的脆弱性

计算机系统的硬件和软件故障可影响系统的正常运行，严重时系统会停止工作。系统的硬件故障通常有硬盘故障、电源故障、芯片主板故障、驱动器故障等；系统的软件故障通常有操作系统故障、应用软件故障和驱动程序故障等。

3. 电磁泄露

计算机网络中的网络端口、传输线路和各种处理机都有可能因屏蔽不严或未屏蔽而造成电磁信息辐射，从而造成有用信息甚至机密信息泄露。

4. 数据的可访问性

进入系统的用户可方便地复制系统数据而不留任何痕迹；网络用户在一定的条件下，可以访问系统中的所有数据，并可将其复制、删除或破坏掉。

5. 通信系统和通信协议的弱点

网络系统的通信线路面对各种威胁显得非常脆弱，非法用户可对线路进行物理破坏、搭线窃听、通过未保护的外部线路访问系统内部信息等。

通信协议 TCP/IP 及 FTP、E-mail、NFS、WWW 等应用协议都存在安全漏洞，如 FTP 的匿名服务浪费系统资源；E-mail 中潜伏着电子炸弹、病毒等威胁互联网安全；WWW 中使用的通用网关接口(CGI)程序、Java Applet 程序和 SSI(supplemental security income)等都可能成为黑客的工具；黑客可采用 Sock、TCP 预测或远程访问直接扫描等攻击防火墙。

6. 数据库系统的脆弱性

由于数据库管理系统(DBMS)对数据库的管理是建立在分级管理的概念上，因此，DBMS 的安全必须与操作系统的安全配套，这无疑是一个先天的不足之处。

黑客通过探访工具可强行登录和越权使用数据库数据，可能会带来巨大损失；数据加密往往与 DBMS 的功能发生冲突或影响数据库的运行效率。

由于浏览器/服务器(B/S)结构中的应用程序直接对数据库进行操作，所以，使用 B/S 结构的网络应用程序的某些缺陷可能威胁数据库的安全。

7. 网络存储介质的脆弱

各种存储器中存储大量的信息，这些存储介质很容易被盗窃或损坏，造成信息的丢失；存储器中的信息也很容易被复制而不留痕迹。

此外，网络系统的脆弱性还表现为保密的困难性、介质的剩磁效应和信息的聚生性等。

1.2.2 网络系统的威胁

网络系统面临的威胁主要来自外部的人为影响和自然环境的影响，它们包括对网络设备的威胁和对网络中信息的威胁。这些威胁的主要表现为非法授权访问、信息泄露、假冒合法用户、病毒破坏、线路窃听、黑客入侵、干扰系统正常运行、修改或删除数据等。这些威胁大致可分为无意威胁和故意威胁两大类。

1. 无意威胁

无意威胁是在无预谋的情况下破坏系统的安全性、可靠性或信息的完整性。无意威胁主要是由一些偶然因素引起，如软、硬件的性能失常、人为误操作、电源故障和自然灾害等。

人为的失误现象有：人为误操作，管理不善而造成系统信息丢失、设备被盗、发生火灾、水灾，安全设置不当而留下的安全漏洞，用户口令不慎暴露，信息资源共享设置不当而被非法用户访问等。

自然灾害威胁如地震、风暴、泥石流、洪水、闪电雷击、虫鼠害及高温、各种污染等构成的

威胁。

2. 故意威胁

故意威胁实际上就是“人为攻击”。由于网络本身存在脆弱性，因此总有某些人或某些组织想方设法利用网络系统达到某种目的，如从事工业、商业或军事情报搜集工作的“间谍”，对相应领域的网络信息是最感兴趣的，他们对网络系统的安全构成了主要威胁。

攻击者对系统的攻击范围可从随便浏览信息到使用特殊技术对系统进行攻击，以便得到有针对性的信息。这些攻击又可分为被动攻击和主动攻击。

被动攻击是指攻击者只通过监听网络线路上的信息流而获得信息内容；或获得信息的长度、传输频率等特征，以便进行信息流量分析攻击。被动攻击不干扰信息的正常流动，如被动地搭线窃听或非授权地阅读信息。被动攻击破坏了信息的保密性。

主动攻击是指攻击者对传输中的信息或存储的信息进行各种非法处理，有选择地更改、插入、延迟、删除或复制这些信息。主动攻击常用的方法有篡改程序及数据、假冒合法用户入侵系统、破坏软件和数据、中断系统正常运行、传播计算机病毒、耗尽系统的服务资源而造成拒绝服务等。主动攻击的破坏力很大，它直接威胁网络系统的可靠性、信息的保密性、完整性和可用性。

被动攻击不容易被检测到，因为它没有影响信息的正常传输，发送和接收双方均不容易觉察。但被动攻击却容易防止，只要采用加密技术将传输的信息加密，即使该信息被窃取，非法接收者也不能识别信息的内容。

主动攻击较容易被检测到，但却难于防止。因为正常传输的信息被篡改或被伪造，接收方根据经验和规律能容易地觉察出来。除采用加密技术外，还要采用鉴别技术和其他保护机制和措施，才能有效地防止主动攻击。

被动攻击和主动攻击有以下 4 种具体类型。

(1) 窃取(interception)：攻击者未经授权浏览了信息资源。这是对信息保密性的威胁，例如通过搭线捕获线路上传输的数据等。

(2) 中断(interruption)：攻击者中断正常的信息传输，使接收方收不到信息，正常的信息变得无用或无法利用，这是对信息可用性的威胁，例如破坏存储介质、切断通信线路、侵犯文件管理系统等。

(3) 篡改(modification)：攻击者未经授权而访问了信息资源，并篡改了信息。这是对信息完整性的威胁，例如修改文件中的数据、改变程序功能、修改传输的报文内容等。

(4) 伪造(fabrication)：攻击者在系统中加入了伪造的内容。这也是对数据完整性的威胁，如向网络用户发送虚假信息、在文件中插入伪造记录等。

1.2.3 Internet 上的危险

Internet 上存在着各种各样的危险，这些危险有恶意的(如故意偷取企业机密、毁坏企业数据等)，也有非恶意的(如因失误而造成的事故)。Internet 上的危险不仅来自于外部，有时也来自内部。虽然在 Internet 上存在不同程度的危险，但为了企业的业务发展，很多企业不得不把企业的内部网与 Internet 互联，向雇员提供 Internet 的访问。

比较典型的 Internet 危险主要有如下几个方面。

（1）软硬件设计故障导致网络瘫痪。如防火墙意外瘫痪而导致失效，以致安全设置形同虚设；由于内外部人员同时访问导致服务器负载过大以致死机，严重者导致数据丢失等。

（2）黑客入侵。一些不怀好意的人强行闯入企业内部网实施破坏；冒充合法的用户进入企业网内部，偷盗企业机密信息和破坏企业形象等。

（3）敏感信息泄露。导致敏感信息泄露的原因如寻径错误的电子邮件、配置错误的访问控制列表，没有设置好不同用户的访问权限等。有时网管员对安全权限设置不当，导致某些有恶意的人故意破坏企业商业机密信息的完整性，以及向竞争对手故意泄露商业机密等。

Internet 之所以存在危险的因素，主要是因为 Internet 本身存在安全漏洞。在设计之初，设计者根本就没想到 Internet 会普及和发展到现在这种程度。在开发 TCP/IP 协议时，主要考虑的是数据的共享，忽略了数据安全。因此 Internet 危险产生的原因如下。

- 不同厂商不同标准的产品集成在网络中引起配置的复杂性。具体说就是网络安全控制由于各种各样的硬件产品与软件产品的加入使安全配置变得异常复杂，很容易出现配置错误或失误，以致导致未经授权的访问。
- 缺乏相应的总体考虑。有些网络在进行系统配置时，无意识地扩大了 Internet 的访问范围，没有意识到某些 Internet 服务会被滥用，许多企业网所允许的访问服务类型过多，不能对一些可能会对入侵者有所帮助的网络信息加以访问限制。
- TCP/IP 协议本身固有的缺陷。TCP/IP 本身存在一些缺陷，一些有经验的黑客很容易利用 TCP/IP 的缺陷攻击企业网。
- 大部分数据没有加密。企业数据在传递过程中很少有加密的，现在有很多现成的软件都能对此进行半路拦截。

1.3　网络风险与安全评估

1.3.1　网络风险评估

定期地对企业的安全工作进行分析是非常重要的，但同样不可轻视的还包括在这个过程中进行网络风险评估。

1. 网络风险评估的概念

风险评估（risk assessment）是对信息资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用而带来风险的可能性的评估。作为风险管理的基础，风险评估是组织确定信息安全需求的一个重要途径，属于组织信息安全管理体系策划的过程。

网络风险评估包括对来自企业外部和内部的网络风险进行评估。对企业内部的网络风险评估与外部的风险评估使用相同的方法，不过要从访问内网的用户角度来进行。

网络安全在过去一直倾向于采取被动式管理的防护策略，被动式防护所使用的设备及工具也是最省事且直接有效的，例如防火墙、入侵检测等。但在复合式病毒出现后，被动式的防护策略已显得防御力不足，会给企事业单位造成大量的损失。漏洞扫描仪（vulnerability scanner）是网络安全中评估弱点及风险的重要工具，其主要功能是找出网络主机及设备的漏洞、隐藏性风险以及鉴定网络架构的安全程度，可对 SMTP、POP、HTTP、FTP、SNMP、

Telnet、SSH、NFS 等协议及账号密码管理疏失及不当的设定做安全检测。它还可对防火墙、路由器等硬设备以及数据库服务器等进行检测。漏洞扫描后所产生的风险评估安全报告也可以分别提供给管理者及技术人员，管理者风险评估报告仅提供了解整个网络的安全状态及风险程度分析，而技术人员报告则提供每一个弱点说明、修补建议，以及技术人员的修补方法。这样可将隐藏性风险及威胁降至最低，使原本必须大费周折的弱点评估管理工作变得轻松容易。

网络的安全管理是必需的，企业必须先评估现有网络的安全状况，才能充分了解自身网络的安全防御能力，并拟定妥善的网络安全政策，配合适当的防护设备、定期审核并与系统管理制度紧密配合，才能在利用网络高效率的同时，保护网络及资源不至于被破坏或窃取。

一般来说，一个有效的网络风险评估测试方法可以解决以下问题。

- 防火墙配置不当的外部网络拓扑结构。
- 路由器过滤规则和配置。
- 弱认证机制。
- 配置不当或易受攻击的电子邮件和 DNS 服务器。
- 潜在的网络层 Web 服务器漏洞。
- 配置不当的数据库服务器。
- SNMP 核查。
- 易受攻击的 FTP 服务器。

2. 网络风险评估过程

进行网络风险评估可以分为发现(discovery)、设备分析(device profiling)、扫描(scanning)和确认(validation)4 个过程。

(1) 发现

发现过程要完成的任务是为要进行评估的网络建立一个档案。这个档案中将包括所有活动设备的地址和与它们相关的 TCP、UDP 和其他内部网络可访问的服务。

在该过程中，可以同时使用主动式和被动式嗅探器来收集网络流量，以备进行分解和分析。通过这种方法获得的信息应当包括活动主机的身份证明、认证证书(诸如用户名和密码组合)、潜在的计算机蠕虫或木马发作的迹象和其他漏洞。

该过程的常见工具有 Nmap(一个网络服务端口扫描器，它使用不同的技术来躲避网络 IDS 的检测)、Ethereal(一个被动式网络嗅探器，支持捕获和解释数据链接层、网络层和应用层的协议数据)、Firewalk(一种高级路由跟踪工具，它使用类似路由跟踪技术来分析 IP 数据包的反馈，以确定网关 ACL 过滤器类型和网络结构)和 hping(一个基于命令行的 TCP/IP 工具，具有防火墙探测、高级端口扫描、网络测试、高级路由等功能)。

(2) 设备分析

在设备分析阶段，通过使用前一阶段所收集的数据信息，能分析出一个列表，其中包括可访问的网络服务、IP 协议堆栈特征及网络体系架构。通过这些信息，可以确定在网络架构中的每一台设备所扮演的角色和相互信任关系。

(3) 扫描

针对前两个过程中发现的每一个网络服务进行已知安全漏洞的测试，这就是扫描过程。

一般来说，这些安全漏洞可以归为一类或几类，其中包括系统漏洞、未授权数据访问、信息泄露、命令执行和拒绝服务（DoS）。在某些情况下，针对一个特定的网络服务可以通过使用 Nessus、nikto 等软件来检测（扫描）与其相关的安全风险。

（4）确认

完成网络风险评估前三个过程的工作后，就要确认漏洞扫描阶段得到的所有结果。确认过程应用的测试和技巧往往专门针对所探测到的安全漏洞。通过该阶段将得到本次网络风险评估的最后结果。

1.3.2 网络安全评估

通过对网络系统进行全面、充分、有效的安全评估，能够快速检测出网络上存在的安全隐患、网络系统中存在的安全漏洞、网络系统的抗攻击能力等。根据对网络业务的安全需求、安全策略和安全目标的评估结果，提出合理的安全防护措施建议。

网络安全评估主要包括以下内容。

1. 安全策略评估

（1）根据网络系统的规划和设计文档、安全需求分析文档、网络安全风险评估文档和安全目标，来评估网络安全策略的有效性。

（2）可采用专家分析的方法，主要评估安全策略是否满足安全需求、是否能够实现安全目标、安全策略是否有效、是否容易实现、是否符合安全设计原则、各安全策略是否一致等。

（3）根据评估结果描述安全策略的完整性、准确性和一致性。

2. 网络物理安全评估

（1）网络物理安全评估的项目包括网络基础设施、配电系统，以及服务器、交换机、路由器、配线柜、主机房、工作站、工作间和记录媒体等硬件设备。

（2）可采用专家分析法，主要评估以上各类设备对物理访问控制（包括安全隔离、门禁控制、访问权限和时限、访问登记等）、安全防护措施（防盗、防水、防火、防震等）和备份（安全恢复中需要的重要部件的备份）的要求是否实现、是否满足安全需求。

（3）根据评估结果描述网络系统的物理安全情况。

3. 网络隔离的安全性评估

（1）网络隔离的安全性评估项目包括网络系统内部与外部的隔离安全性、内部虚网划分和网段划分的安全性和远程连接（VPN、Modem）的安全性。

（2）可采用侦听工具评估防火墙过滤和交换机、路由器实现虚网划分的情况；采用漏洞扫描软件评估防火墙、交换机和路由器是否存在安全漏洞。

（3）根据评估结果描述网络隔离的安全性。

4. 系统配置的安全性评估

（1）系统配置安全性的评估项目有各网络设备（路由器、交换机、Hub）的网管代理是否修改了默认值，是否有措施保证普通用户不能远程登录路由器、交换机等网络设备，服务模

式的设置，服务软件版本的更新，操作系统的漏洞和设备的安全性。

（2）可采用漏洞扫描软件，测试操作系统存在哪些漏洞；检查网络系统采用的各设备是否采用了安全性得到认证的产品；根据设计文档，检查网络系统配置是否被更改和更改原因等是否满足安全需求。

（3）根据评估结果描述网络系统配置的安全状况。

5. 网络防护能力评估

（1）网络防护能力的评估内容包括对拒绝服务、电子欺骗、网络侦听、入侵等攻击形式是否采取了相应的防护措施及防护措施是否有效。

（2）可采用模拟攻击、漏洞扫描软件等评估网络的防护能力。

（3）根据评估结果描述网络的防护能力。

6. 网络服务的安全性评估

（1）网络服务的安全性评估项目有服务隔离的安全性（根据信息敏感级别要求是否实现不同服务的隔离）和服务的脆弱性分析（主要测试系统开放的服务是否存在安全漏洞）。

（2）可采用漏洞扫描软件，测试网络系统开放的服务是否存在安全漏洞；模拟各服务的实现条件，检测服务的运行情况。

（3）根据评估结果描述网络服务的安全性。

7. 网络应用系统的安全性评估

（1）网络应用系统的安全性评估项目包括应用程序是否存在安全漏洞，应用系统的访问授权、访问控制等防护措施的安全性。

（2）主要采用专家分析和模拟测试的方法进行网络应用系统的安全性评估。

（3）根据评估结果描述系统应用程序的安全性。

8. 病毒防护安全性评估

（1）采用专家分析和模拟评估来检测服务器、工作站和网络系统是否配备了有效的病毒检测软件和病毒清查的执行情况。

（2）根据评估结果描述对病毒防护的安全性。

9. 备份的安全性评估

（1）备份的安全性评估项目有备份方式的有效性、备份的充分性、备份存储的安全性和备份的访问控制。

（2）可采用专家分析的方法，根据系统的安全需求、业务的连续性计划来评估备份的安全性。

（3）根据评估结果描述备份系统的安全性。

10. 紧急事件响应能力评估

（1）紧急事件响应能力评估项目包括是否有紧急事件响应程序、响应程序是否有效以

及平时的准备情况(备份和演练)等。

(2) 可模拟紧急事件响应条件,检测紧急响应程序是否能够有序、有效地处理安全事件。

(3) 根据评估结果,描述紧急事件响应程序的充分性和有效性。

1.4 网络安全的策略与措施

网络信息系统是一个复杂的计算机系统,它本身在物理、操作和管理上的种种漏洞构成了系统的安全脆弱性,尤其是多用户网络系统自身的复杂性、资源共享性,使单纯的技术保护防不胜防。攻击者使用的"最易渗透原则",必然在系统中最薄弱的地方进行攻击。因此,充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测是设计信息安全系统的必要前提条件。

网络安全涉及人、技术、操作等要素,单靠技术或管理都不可能实现。因此,必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。切忌只重视其中一种而忽视另一种的情况出现,要明白好的技术是管理的基础,而高效的管理则是技术强有力的保证。可采取相应的网络安全策略来实现网络安全。这不但要靠法律的约束、安全的管理和教育,更重要的是要靠先进的网络安全技术支持。

先进的网络安全技术是网络安全的根本保证。用户对自身面临的威胁进行风险评估,决定其所需要的安全服务种类,选择相应的安全机制,再集成先进的安全技术,就形成一个可信赖的安全系统。网络的安全策略一般包括安全立法、安全管理、物理(实体)安全、访问控制、信息保密和安全审计等方面,每一项策略可由多项措施来实现。

1.4.1 网络安全立法

计算机犯罪是一种高技术犯罪活动,也是未来社会的主要犯罪形式之一,因此,面对日益严重的计算机犯罪,必须建立相关的法律、法规进行约束。通过建立国际、国内和地方计算机信息安全法来减少计算机犯罪案(如盗窃网络设施、非法侵入网络来破坏和盗窃信息资源、故意制造病毒破坏网络系统等)的发生。由于法律具有强制性、规范性、公正性、威慑性和权威性,因此它在很多方面具有不可替代的作用。制定并实施计算机信息安全法律,加强对计算机网络安全的宏观控制,对危害计算机网络安全的行为进行制裁,为网络信息系统提供一个良好的社会环境是十分必要的。

1. 国外的计算机信息安全立法

在国际上,由于发达国家的计算机应用已非常普及,因此,其计算机安全立法工作也早已进行。不同形式的法律,如《计算机安全法》、《信息自由法》、《伪造访问设备和计算机欺骗与滥用法》、《数据保护法》、《计算机犯罪法》、《计算机软件保护法》、《电子资金转账法》、《保密法》、《个人隐私法》等均已出台,一些国家还将计算机犯罪与刑法、民法联系在一起,修改有关条款,颁布实施,收到了较好的效果。

2. 我国的计算机信息安全立法

我国的计算机信息安全立法模式基本上属于“渗透型”,国家未制定统一的计算机信息安全法,而是将涉及信息安全的法律规范渗透和融入相关法律、行政法规、部门规章和地方法规中,初步形成了由不同法律效力层构成的计算机信息安全法律规范体系。

我国信息安全立法有四个层次:一是由全国人大常委会通过的法律,除《警察法》、《刑法》、《保守国家秘密法》外,涉及计算机信息安全的法律还有《全国人大常委会关于维护互联网安全的决定》等;二是国务院为执行宪法和法律而制定的行政法规,主要有《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》和《互联网上网服务营业场所管理条例》等;三是国务院各部委根据法律和行政法规在本部门权限范围内制定的规章及规范性文件,主要有《计算机病毒防治管理办法》、《互联网电子公告服务管理规定》、《国际互联网出入信道管理办法》、《中国互联网络域名注册实施细则》、《互联网信息服务管理办法》等;四是各省、市、自治区制定的地方性法规,如《××省计算机信息系统安全保护管理规定》等。

我国缔约或参加的有关计算机及网络信息的国际公约有《建立世界知识产权组织公约》、《保护文化艺术作品的伯尔尼公约》、《世界版权公约》、《与贸易有关的知识产权(包括假冒商品贸易)协议》等。

1.4.2 网络安全管理

安全管理和安全技术措施是相辅相成的,因此在网络安全中,在实施技术性安全措施进行的同时,必须考虑安全管理措施。因为诸多的不安全因素恰恰反映在组织管理和人员使用方面,而这又是计算机网络安全所必须考虑的基本问题,所以应引起各计算机网络应用部门领导的重视。加强网络的安全管理、制定有关规章制度,对于确保网络的安全、可靠运行起到十分有效的作用。网络安全管理包括确定安全管理等级和安全管理范围、制定有关网络操作使用规程和人员出入机房管理制度、制定网络系统的维护制度和应急措施等。

各计算机网络使用机构、企业或单位,应建立相应的网络安全管理制度,加强内部管理,建立合适的网络安全管理系统和安全审计与跟踪机制,提高整体网络的安全体系。

因此,网络系统应设立专门的安全管理机构和人员,负责网络所有日常安全管理活动,如监视全网运行和安全告警信息、网络各个层次的审计与日志信息的常规分析、安全设备的常规设置与维护、网络系统安全策略的规划制定与实施和网络安全事件的处理等。

网络安全管理措施包括建立健全安全管理机构、行政人事管理和系统安全管理制度等。

1. 安全管理机构

为保证计算机网络系统的安全运行,网络系统的使用单位应当成立计算机安全管理机构,设立专职安全人员。这些安全人员包括安全管理、安全审计、系统分析、软硬件管理、通信及保安人员等。

网络安全管理机构的设置与系统的规模直接相关。若是一个庞大系统,且终端客户遍布世界各地,则在每个区域内都应有一个这样的管理机构。所以,一个网络系统设置多少安全管理机构是不定的,但机构中各有关方面人员的职责是固定的。

2. 安全行政人事管理

对计算机网络信息系统的大部分威胁都来自人为因素。因此，无论系统如何自动化，总是由人设计和操作使用的。而人本身是很复杂的，是有感情的，受自身生理和心理因素的影响和制约，有时为了达到某种目的而不惜铤而走险，利用计算机系统进行犯罪活动。据研究表明，从事计算机职业犯罪的人员中，70％是信息系统运行和管理人员。因此，对信息系统的运行和管理人员进行教育、奖惩、培养和训练，加强行政和人事管理，保证网络信息安全和保密是非常必要的。

行政人事管理的职责是制定严格的人事管理、岗位分工、奖惩分明和责任追究等规章制度，使网络系统工作人员做到各司其职、各负其责、互相监督和制约，保证系统安全运行。

3. 系统安全管理

一般来说，网络系统的安全管理主要是确定安全管理原则和相应的安全管理制度。网络系统安全管理机构应根据多人负责制、职责分离、任期有限和最小权限等原则，制定相应的管理制度或规范。

(1) 确定网络系统的安全等级，根据系统的安全等级，确定系统的安全管理范围。对安全等级要求较高的系统，要进行分区控制，限制工作人员出入与己无关的区域；人员的出入管理可采用身份证件识别或安装自动识别登记系统，采用磁卡、身份卡等手段对出入人员进行识别和登记。

(2) 制定安全管理制度，如制定计算机机房安全管理制度、机房设备和数据管理制度等。

(3) 还要有对操作系统和数据库的访问的监控措施，制定严格的操作规程，制定完备的系统维护制度、计算机网络系统的灾害处理对策、灾难恢复计划和具体恢复措施等。

1.4.3　物理(实体)安全

网络实体是指除一些实际存在的物体和设备外，还包括客观存在的与某一应用有关的事物，如含有一个或多个程序、进程或作业之类的成分。即实体既包括硬件实体(如某一设备、某一接口芯片)，也包括软件实体(如程序)。网络实体安全保护就是指采取一定措施对网络的硬件系统、数据和软件系统等实体进行保护和对自然与人为灾害进行防御。

网络实体安全就是保护计算机网络设备、设施和其他媒体免遭自然灾害(如地震、水灾、雷电、风暴等)和人为灾害(人为操作失误或错误及各种计算机犯罪行为)导致的破坏。网络实体安全是整个计算机网络系统安全的前提，它主要包括网络环境安全(对系统所在环境的安全保护，如机房安全保护和灾难保护)、网络设备设施安全(包括设备的防盗、防毁，对抗通信链路上的窃听、篡改、流量分析攻击，抗电磁干扰及电源保护等)、媒体安全(包括媒体数据的安全及媒体本身的安全)。为保证网络系统的物理安全，还要防止系统信息在空间的扩散。通常是在物理上采取一定的防护措施来减少或干扰扩散出去的空间信号，如在产品保障方面、运行安全方面、防电磁辐射泄露方面和安保方面。

对网络硬件、操作系统、网络数据和软件的安全保护，对网络病毒、黑客攻击的防范等详见第 2 章、第 3 章和第 6 章。

1.4.4 访问控制

访问控制就是规定哪些用户可访问网络系统，对要求入网的用户进行身份验证和确认，这些用户能访问系统的哪些资源，他们对于这些资源能使用到什么程度等问题。访问控制的基本任务就是保证网络系统中所有的访问操作都是经过认可的、合法的，防止非法用户进入网络和合法用户对网络系统资源的非授权访问。

访问控制安全措施涉及口令安全、入网限制、认证和授权、数字签名、非否认、防火墙、入侵检测、网络扫描和监听等技术。利用上述技术或措施对网络用户身份进行验证和确认，规定不同软件及数据资源的属性和访问权限，进行网络监视、设置网络审计和跟踪、使用防火墙系统、入侵检测和防护系统等方法实现访问控制安全。

涉及网络访问控制安全的相关内容详见第3～6章。

1.4.5 数据保密

数据加密保护就是采取一定措施，对网络系统中存储的数据和在线路上传输的数据进行变换（加密），使得变换后的数据不能被无关的用户识别，保证数据的保密性。数据加密的目的是隐蔽和保护具有一定密级的信息，既可以用于信息存储，也可以用于信息传输，使其不被非授权方识别。数据加密是提高计算机网络中信息的保密性、完整性，防止机密信息被破译所采用的主要技术手段，也是最可靠、最直接的方案。

数据加密保护通常是采用密码技术对信息（数据和程序）进行加密、数字签名、用户验证和非否认鉴别等措施实现的。数据加密算法主要有对称密钥加密和非对称密钥加密两种。

数据加密技术是所有信息安全保密技术的基础。与数据保密技术相关的内容详见第4章、第5章和第8章等。

1.4.6 网络安全审计

安全审计是记录用户使用计算机网络系统进行所有活动的过程，它不仅能够识别谁访问了系统，还能指出系统正被怎样地使用。同时，系统事件的记录能够更迅速和系统地识别问题，并且是后面阶段事故处理的重要依据，为网络犯罪行为及泄密行为提供取证基础。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据。

安全审计是识别与防止网络攻击、追查网络泄密行为的重要措施之一，是安全网络必须支持的、提高网络安全性的重要手段。安全审计具体包括两方面的内容：一是采用网络监控与入侵防范系统，识别网络各种违规操作与攻击行为，即时响应（如报警）并进行阻断；二是对信息内容的审计，可以防止内部机密或敏感信息的非法泄露。

网络安全审计措施可通过多层次的审计手段实现。具体而言，网络的安全审计系统应由网络层安全审计、系统安全审计和信息内容的安全审计三个层次组成。网络层安全审计主要利用防火墙的审计功能、网络监控与入侵检测系统来实现。系统安全审计主要是利用各种操作系统和应用软件系统的审计功能实现，包括用户访问时间、操作记录、系统运行信息、资源占用等。

1.5　网络系统的日常安全管理

对于网络系统的安全管理和维护，不仅需要有配套的安全防御措施，还需要规范的管理制度和流程，更需要高素质的安全管理和操作人员。

1.5.1　网络系统的日常管理

一般网络管理人员所面对的网络管理环境大都已经采取了某些安全措施，构成了一定的防御体系。同时，从管理的角度讲，比较重视网络安全的企业或事业单位，都设有专门的安全管理机构，制定了相应的安全制度和规范。从网络管理人员的素质讲，一般都具有一定的安全技能，如分析日志、了解攻击特点、熟悉各类操作系统以及本网络的拓扑、IP 分配情况、设备配置情况、系统配置情况、应用系统情况。但这些还远远没有达到网络安全日常维护的要求。

网络系统的安全维护通常有以下几个方面。

1．口令（密码）管理

口令问题容易被人忽视。许多系统建设得非常完美，但在口令管理上不够严格，甚至漏洞百出。试想，即便是世界上最坚固的保险柜，如果其密码是 0000，那么这个坚固的躯壳就成为摆设了。

一般网络工作人员常犯的口令错误有：多个账号使用同一个密码；密码全部采用数字组合或字母组合；密码从不更新；密码被记录于易见的媒体上；远程登录系统时，账号和密码在网络中以明文形式传输等。

作为网络安全管理人员，在口令管理上应该养成好习惯，比如：选取数字、字母、符号相间的口令；口令不随便书写在易见的媒体上；适时更新口令；及时删除已撤销的账号和口令；远程登录时使用加密口令；更严格情况可采用口令鉴别和 PKI 验证过程。

2．病毒防护

建议网络系统的所有计算机都安装统一的网络防病毒软件，这样容易解决病毒库的及时升级问题。通过对防病毒服务器进行及时升级，可以做到众多的客户端病毒库及时升级，这样可对最新的病毒进行及时防杀，减少病毒危害。

对于作为服务器的主机，无论是使用 Windows 操作系统还是非 Windows 操作系统，防病毒软件对于主机系统的性能都会有不同程度的影响。但是，网络防病毒软件还是要尽可能地覆盖所有的主机，并及时进行病毒库升级。在日常维护中，最好是每隔两三天就检查一次是否需要升级病毒库，在必要时及时进行升级。

谈到病毒防护，不要以为防病毒软件对任何病毒都有作用。防病毒软件并不能防杀掉所有类型的病毒，比如蠕虫病毒。造成这种情况的原因很多，如用户没有及时升级病毒，或者该病毒的特征定义不准确等。蠕虫病毒带有黑客攻击性质，对于黑客攻击特征的研究，可以借助于入侵检测系统等监控设备，进行及时监控，找到有问题的机器，及时修补漏洞。

3. 漏洞扫描

网络管理员应密切跟踪最新的漏洞和攻击技术，及时对网络设备进行加固。如果及时对 IIS 打补丁，就不会发生红色代码蠕虫问题；如果及时对 SQL Server 打补丁，就不会发生 SQL 蠕虫问题；如果及时加强口令的控制，关闭不必要的服务，就不会发生被他人远程控制问题；如果在出口进行源路由控制，就不会有 DDoS（分布式拒绝服务）攻击从本网发动等问题。

通过漏洞扫描系统对网络设备进行扫描，可以从设备之外的网络角度来审视网络上还有哪些漏洞没有修补，正在提供什么样的服务，以此找到需要关闭的服务，甚至也可以发现部分密码设置过于简单的账号。

建立一个列表，列出网络中所有主机应该提供的服务和端口，使用扫描系统，检查每台主机，看是否有不必要的服务没有关闭，或有漏洞的地方，及时做出调整及修补。如果有计算机被人利用，应启动应急响应流程，分析原因，找到攻击者使用的方法；必要时，需要对全网安全策略进行调整。在日常维护中，每十天左右可对重要的主机进行一次扫描。由于扫描要占用带宽，可根据带宽情况和设备数量，合理调整扫描周期和时间。

4. 边界控制

边界可理解为所管辖的内部网与外部网的连接，如连接 Internet 的边界，连接第三方网络的边界；也可以理解为在一个广域网中，各局域网之间的连接边界。

网络之间的连接设备一般都是路由器，为了加强安全控制，通常在路由器上配备防火软件，使之构成网络层防火墙。当然，网络之间可能还有其他类型的隔离设备，如网闸等。在加强对路由器、防火墙本身的安全控制之外，也要利用这些设备对边界访问进行控制，特别是连接 Internet 的边界。事实上，网络管理员没有足够的能力去管理 Internet 上的行为，但有足够的权限控制所辖内部网络。边界访问控制得比较好，就能有效地减少来自 Internet 的攻击风险。比如，在路由器上采用访问列表来控制内外的访问，采用源路由器控制方法，过滤非本地的 IP 报文发送到 Internet 上，可避免黑客的 IP 欺骗，也可控制发自本网络内部的伪造源地址的蠕虫病毒和 DDoS 攻击。

加强局域网之间的边界控制，可以减少攻击威胁的范围。比如，SQL 蠕虫病毒在某局域网内爆发，由于边界控制设备关闭了 SQL Server 连接的端口，因此，至少可以避免该病毒从本局域网传染到其他局域网。

5. 实时监控

以上措施都能提高网络的组成元素的安全强度，但这还不够。因为网络访问是动态的，网络管理员要时时刻刻监视网络的访问情况，特别是密切注意潜在的攻击行为，采取必要手段进行及时控制；对已攻击成功的事件，应启动应急响应流程，分析黑客是利用了网络中的哪些薄弱环节，使用什么攻击方式进行的，考虑应如何调整和加强安全措施等。

利用入侵检测系统（IDS）建立全网的监控系统，即可以实施对网络的实时全面监控，也可以对某个或某些安全事件进行特别监控。管理员要充分利用事件的自定义功能，将自己认为有必要监控的网络访问进行自定义。在日常网络的安全维护中，应根据实际情况，实行

每周 7 天的全天候(7 天×24 小时/天)监控或 5 天×8 小时/天监控。

6. 日志审核

这里所说的日志是指操作系统日志、应用程序日志和防火墙日志。如果网络范围比较大,设备比较多,日志量就比较大。如果没有专门的日志分析工具,网络管理员应只对特别重要的服务器日志进行常规的日志分析。通过这些分析,可以发现服务器上是否有异常活动。日志分析审核是对网络安全监控系统的一个补充,在日常维护中,建议每月进行一次。

7. 应急响应

采取再多的安全措施,也不会造就绝对安全的网络系统。在网络安全方面,“攻”和“防”是一对既互相对立又互相促进的矛盾体,它们总是在实践过程的不断较量中相互制约和不断发展的,往往是先有新的“攻击”手段和方法出现,随后再有相应的“防御”措施出台,正所谓“道高一尺,魔高一丈”。因此,在攻击者侵入网络后,需要有及时的应急响应措施,对安全事件进行分析和追踪,实施修补。

希望每个较大的网络系统安全管理员都建立自己的紧急响应流程,使所有安全管理人员都知道,在出现紧急安全事件时应如何处理。如果暂不具备对安全事件分析的实力,可由有能力提供紧急响应安全服务的服务提供商进行支持。此外,应及时对每次应急响应进行总结,修正应急响应流程。

8. 软件和数据文件的保护

软件和数据文件包括系统软件、应用软件及应用系统的数据库各项文件等。操作系统软件的安全性体现在对程序保护的支持和对内存保护的支持上。在现代信息系统中,硬件对操作系统的支持比较完善,如使用硬件技术中的特权指令、重定位和界限寄存器、分页、分段等功能实现对资源的合理分配,将用户的程序和数据管理起来,避免相互间的干扰和分时冲突。

在虚拟存储技术中采用段页表进行地址映射,在这些表中规定了对内存信息的访问权限。操作系统正是由内存管理程序对内存资源进行控制和保护的。因为操作系统管理了系统的全部资源,因此它必须避免一般用户的进入。因该特定入口是由管理程序控制的,所以当一般用户试图通过特定入口(陷阱)向操作系统请求服务时,就无法进入该管理程序。对于多进程的系统,可以采取优先级控制的方法防止进程之间的干扰和对系统区的非法访问。

目前,各种应用软件、软件工具和数据文件的数量正以惊人的速度增长,以满足日益增长的计算机应用的需要,但非法复制、非授权侵入和修改是对软件(数据文件)的主要危害。从销售商的角度看,需要一些保护措施防止销售的软件被非法复制。非法复制除给软件销售商带来经济损失外,更重要的是,一旦对国家经济、工商、金融、外贸以及军政部门的机密软件和系统软件(文件)进行非法复制,将造成不可估量的损失,甚至威胁到国家安全。

通常采用市场策略、技术策略和法律策略三种保护策略对付软件的非法复制。

(1) 市场策略

比较典型的市场策略是对软件商品标以诱人的低廉价格,使每个潜在用户都愿意购买它,因为购买后还可以得到所需文件和后续的技术支持。

(2) 技术策略

技术策略涉及较多具体的软件保护技术,如抗软件分析法、唯一签名法、软件加密法和数据加密法等。抗软件分析法可使攻击者不能动态跟踪与分析软件程序。唯一签名法可保证软件不被非法复制。但随着科学技术的不断发展,各种各样的复制软件工具不断出现,攻击者可以通过复制软件的源代码进行静态分析。为防止这种静态分析,可对整个程序或程序的关键部分进行加密。软件加密是将介质上存储的程序代码变换成一种密文形式,使得攻击者即使是复制了该软件也无法读懂它,因而也就无法分析和使用它。

(3) 法律策略

利用软件保护法等相应的法律法规的约束和威慑力,使一些人对非法侵权有所顾忌,不得不去购买正版软件。虽然法律本身的作用是有限的,但把几种策略结合起来使用还是有效的。

1.5.2 网络日志管理

网络日志不仅能用来进行安全检查,而且还能够帮助用户更好地从事网络管理工作。网络管理员的一个十分重要的工作就是做好网络日志,有效地利用网络日志进行网络安全管理是一项十分重要的工作。

在网络系统里,日志管理是一个非常重要的功能组成部分。它可以记录下系统所产生的所有行为,并按照某种规范表达出来。管理员可以使用日志系统所记录的信息为系统进行排错,优化系统的性能,或者根据这些信息调整系统的行为。在安全领域,日志管理的重要性更为突出,它是安全审计方面最主要的工具之一。

按照系统类型可将日志分为操作系统日志、应用系统日志、安全系统日志等。每种操作系统的日志都有其自身特有的设计和规范,例如,Windows 系统的日志通常按照其惯有的应用程序、安全和系统这样的分类方式进行存储,而类似 Linux 这样的各种 Class UNIX 系统通常都使用兼容 Syslog 规范的日志系统。应用系统日志主要包括各种应用程序服务器(例如 Web 服务器、FTP 服务器)的日志系统和应用程序自身的日志系统,不同的应用系统都具有根据其自身要求设计的日志系统。安全系统日志从狭义上讲指信息安全方面设备或软件,如防火墙系统的日志,从更广泛的意义上来说,所有为了安全目的所产生的日志都可归入此类。

下面就如何利用网络日志进行网络管理工作做一些简要介绍,并通过一些日常的范例来说明。

1. 网络日志是日常管理的 FAQ

在日常的网络管理工作中,要形成一种习惯,就是将当天遇到的问题与解决方法填写在网络日志中,然后定期地将这些内容进行整理归类到一个名为网络管理的 FAQ(日常问答)中。FAQ 以一问一答的方式收集内容,以 Web 形式共享。这样,当网络管理员此后再遇到问题时,可以先在这里寻找答案,这样可大大提高解决问题、排除故障的效率。

2. 网络日志是排除故障的黑匣子

网络日志对于故障排除也能起到飞机黑匣子的功能。下面通过几个案例来说明网络日

志对排除网络故障的帮助。

例 1-1　某企业内部有一台应用服务器，操作系统是 Windows NT 4.0，在上面运行着一个通信网关程序。有一天网络管理人员一上班就发现这个通信网关程序罢工了。结果一检查，该程序已异常退出，而且再也启动不了。这时，网络管理人员迅速查找网络日志，发现在前一天下班时，另一名网络管理人员为了提高安全性，在该服务器上打了 SP6 补丁，然后关机下班。网络管理人员马上与该程序的开发商取得联系，确认了该程序与 SP6 不兼容，并得到了修改该故障的新版程序，顺利地解决了问题。在本例中，通过查看网络日志，寻找到了变动因素，从而找到了引起该故障的原因。

例 1-2　有一段时间，某企业内部网络出现了一个奇怪的现象，每天中午大家都无法正常收发 E-mail，接收邮件经常超时，数据传输很慢。开始大家认为可能是由于中午上网人多而引起的。为了能够找出原因，网络管理员连续几个中午进行网络流量监测，并将结果记录下来。然后翻开网络日志，查看在发生该情况之前的网络流量数据，结果发现这几天中午的网络流量居然是平时最大值的 10 多倍。他们觉得这样的情况肯定不是上网人数简单增加引起的，就继续进行网络监控，试图寻找出原因。结果用 Sniffer 监听到了一台 PC 在源源不断地向外广播大量的数据包，找到这台 PC 的用户后才知道，该用户在用"超级解霸"看 VCD，当打开他的"超级解霸"时发现他误设置了打开 DVB 数字视频广播，结果在他看 VCD 的同时向整个局域网用户进行了视频广播，因此导致了网络阻塞。试想如果没有网络日志数据，就可能无法得知网络数据的增长到底有多大，是不是与上网人数增加有关系，就可能会盲目地采用增加带宽方式来解决该问题了。

3. 网络日志是网络升级的指示仪

网络日志记录了网络日常运行的状态信息，这些信息显示了网络的动态情况，有了这些情况，就可以正确地做出网络升级的决策，使得网络升级能够落到实处。同时，网络日志还为网络升级提供了详细的数据依据。

例如，每年底企业领导都要求网络管理部门提交一个关于新一年中网络升级的需求报告，这时网络管理员就可打开网络日志，对网络日志中网络流量数据进行分类统计，获取网络流量的增长率、网络流量的高峰时期等信息；对网络中病毒记录进行统计，可以得知现行的病毒防治策略是否有效；还可以从网络日志中发现每一个网络服务器的负载变化情况，再根据这一情况制定网络服务器软硬件的更新。基于网络日志提供的上述各种数据信息，网络管理部门即可制定出一个较完美的升级计划向领导汇报了。

总之，如果行之有效地利用网络日志中的数据记录，将能够帮助网络管理员更好地完成网络管理工作。

4. 网络日志便于系统运行维护管理

以保障系统稳定运行为目的，通过采集各种网络设备、操作系统及系统软件平台的运行日志及各种消息、主动探测运行状态等手段，全面地监测、记录各种平台的动态信息及配置变更，实时地提供报警信息并输出各种综合日志分析报告，为系统管理人员提供了一个监测面广、响应及时、具有强大分析能力的信息系统基础设施——日志监测管理平台，这样可大大降低系统运行维护人员的工作量和定位故障的时间，快速完成系统运行维护任务。

5. 网络设备的日志管理

查看交换机、路由器和其他网络设备的日志,可以帮助网络管理员迅速了解和诊断问题。一些网络管理员认为日志管理是信息安全管理的内容,与系统管理关系不大,这绝对是错误的。很多硬件设备的操作系统也具有独立的日志功能,以Cisco路由器为代表的网络设备通常都具有输出Syslog兼容日志的能力。下面以常见的Cisco设备为例介绍在网络设备日志管理中最基本的日志记录方法与功能。

在Cisco设备管理中,日志消息通常是指Cisco IOS中的系统错误消息,其中每条错误信息都被定一个级别,并伴随一些指示性问题或事件的描述信息。Cisco IOS发送日志消息(包括debug命令的输出)到日志记录。默认情况下,只发送到控制台接口,但也可以将日志记录到路由器内部缓存。在实际管理工作中,一般将日志发送到终端线路,如辅助和虚拟终端连接(virtual type terminal,VTY)线路、系统日志服务器和SNMP管理数据库等。

(1) 基本日志记录的配置

在设置日志记录时,需要完成两个基本的任务:打开日志记录和控制日志在线路上的显示。

① 日志记录

一般地,日志记录只在路由器的终端控制台打开,要在其他地方记录日志,则必须相应地打开日志记录并进行配置。使用logging on命令可打开日志记录,其他的如logging命令,可以为日志记录打开其他已配置的目的地,如系统日志服务器或路由器的内部缓存。在将系统消息记录到除了控制台端口的其他位置之前,必须执行该命令。

② 配置同步日志记录

在路由器线路上显示日志时,可能当用户正在输入命令时,有路由器消息显示在正在输入的命令行中间。虽然这个消息和正在输入的命令无关,可以继续输入来完成命令,但是这种情况是很烦人的。

logging synchronous命令的主要目的是将日志消息输出和调试输出同步到控制台、辅助和VTY线路。当启用这个特性时,同步日志使得Cisco IOS显示消息,然后执行一个等价的Ctrl-R的命令,这使得路由器将已经输入的信息重新显示在命令行上。

在config-line模式下可以使用logging synchronous命令来影响日志消息的显示,如:

```
Router(config-line)# logging synchronous [level severity_level | all [ limit #_of_line ] ]
```

severity_level是指日志消息的严重程度,这些消息是异步显示的。严重性数值比该值高(更低严重性)的消息被同步显示;数值低(更高严重性)的消息被异步显示,默认的严重级别是2。参数all使得所有消息都被异步显示,不管分配的严重级别。参数limit指定在路由器开始丢弃新的消息前,有多少个同步消息可以在队列中排队,默认值是20。如果到达该阈值,路由器必须丢弃新的消息时,就会看到_of_messages due to overflow日志消息。

(2) 日志级别

在讨论将记录日志到其他目的地之前,管理员应当熟悉日志消息和严重级别。每个日志消息被关联一个严重级别,用来分类消息的严重等级:数字越低,消息越严重。严重级别的范围从0(最高)到7(最低)。

(3) 将日志记录到其他位置

① 到逻辑 VTY

有 logging console 和 logging monitor 两个命令可用于控制日志消息发送到路由器的线路上。logging console 命令是指将日志记录到物理的 VTY，如控制台和辅助线路。logging monitor 命令是指将日志记录到逻辑的 VTY，如 Telnet 会话。一般地，记录日志在控制台对所有级别都打开，但是也可以通过改变 logging console 命令中的严重级别来修改。默认情况下，网络设备不会将逻辑 VTY 打开，需要执行 logging monitor 或者 terminal monitor，可将控制台日志消息复制到 VTY。

由于设备需要将消息显示在终端线路上，这样会给网络设备增加额外负担，所以应将严重级别改到比调试更高的严重级别(较低的数字)。

② 内部缓存记录

当日志消息记录到逻辑 VTY 后，依然无法保证调试过程被完整记录下来。比如当用户没在意连接线路的屏幕输出，或消息滚过屏幕并超出了终端软件的历史缓存时，则没有任何机制可以再看到那些丢失的消息。一个解决方法是将日志消息记录到路由器的内部缓存，根据路由器平台的不同，该项可能是默认打开或者关闭的；在大多数平台下，默认是打开的。使用以下命令将日志记录到路由器的缓存：

```
logging buffered [ buffer_size | severity_level ]
```

该命令有两个参数，buffer_size 参数指定应该为内部缓存分配多大的内存，以字节为单位，从 4096 到 294 967 295 字节。使用 default logging buffered 命令可将缓存大小设成出厂的默认值。

值得注意的是，将缓存的大小设置得太大时，如果有很多消息，这会使得路由器耗尽内存，可能使其崩溃。

③ 到日志服务器

将日志记录到日志服务器比将日志记录到命令行或者内部缓存要稍微复杂一些，但这也是 Cisco 和其他厂商推荐的做法。将日志记录到服务器的相关命令如下：

```
logging [host - name | ip - address]
logging trap level
logging facility facility - type
logging source - interface interface - type interface - number
logging on
```

④ 到 SNMP 数据库

可以将日志信息发送到的最后一个地方是 SNMP 管理平台，很多网管软件都有相关的说明。

6. Windows 日志文件的保护

日志文件对网络的安全和管理非常重要，因此要加强对其保护，防止日志文件被删除或非法操作。

（1）修改日志文件存放目录

Windows 日志文件默认路径是%systemroot%\system32\config，可以通过修改注册表来改变它的存储目录，增强对日志的保护。

在菜单中选择“开始”→“运行”，在对话框中输入“Regedit”，按回车键后弹出注册表编辑器，依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog”后，下面的 Application、Security、System 几个子项分别对应应用程序日志、安全日志和系统日志。

以应用程序日志为例，将其转移到“E：ABC”目录下。首先选中 Application 子项，在右栏中找到 File 键，其键值为应用程序日志文件的路径“%SystemRoot%system32configAppEvent.Evt”，将其修改为“E：ABC\AppEvent.Evt”，如图 1.1 所示。接着在 E 盘新建“ABC”目录，将“AppEvent.Evt”复制到该目录下，重新启动系统，这样就完成了应用程序日志文件存放目录的修改，其他类型日志文件路径修改方法相同，只是在不同的子项下操作。

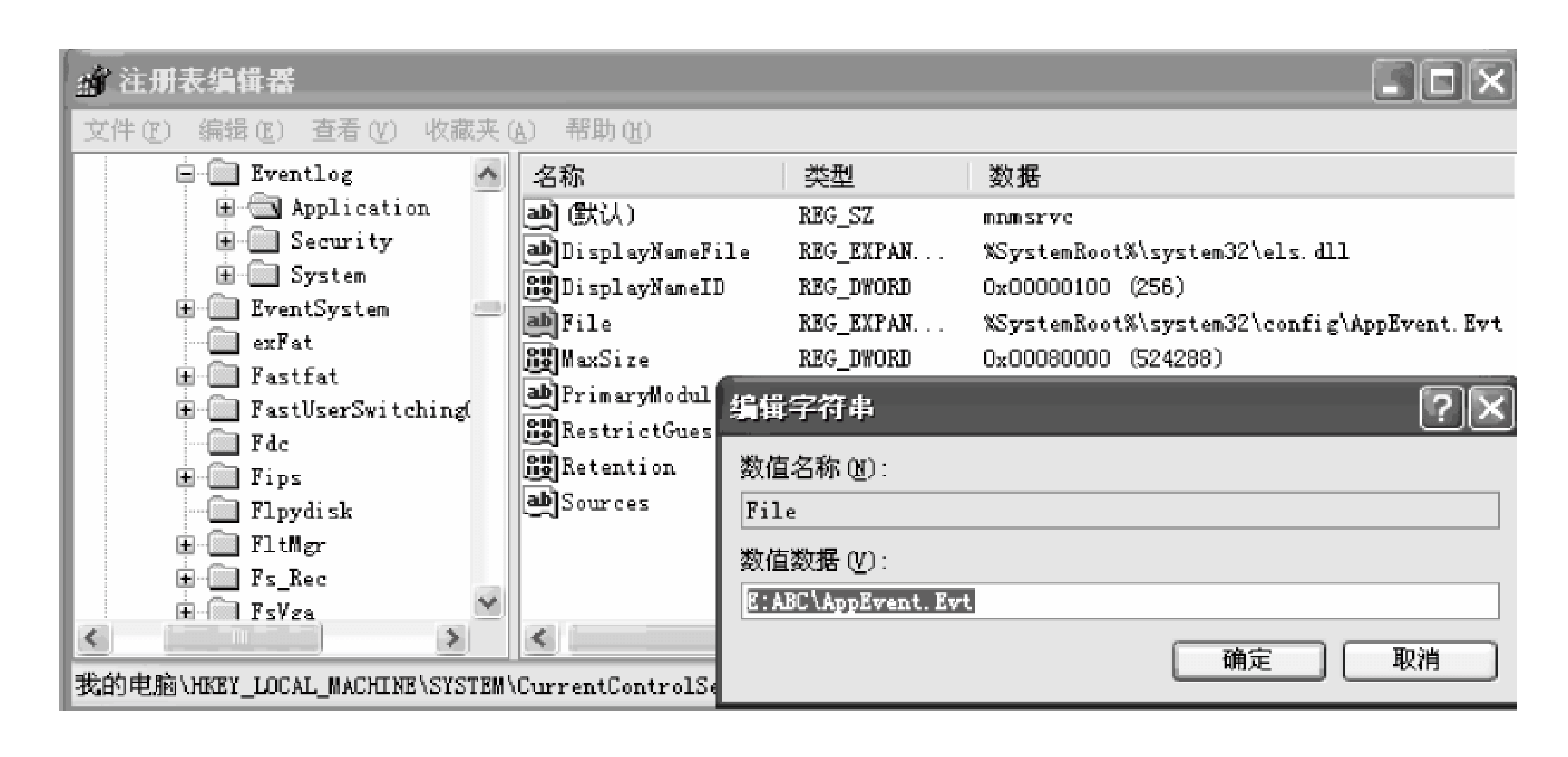


图 1.1 修改日志文件存放目录

（2）设置文件访问权限

修改了日志文件的存放目录后，日志还是可以被删除的。可通过修改日志文件访问权限，防止这种事情发生，前提是 Windows 系统要采用 NTFS 文件系统格式。

在 D 盘的 CCE 目录（共享目录）右击鼠标，选择“属性”，切换到“安全”标签页后，首先取消“允许将来自父系的可继承权限传播给该对象”选项的勾选，接着在账号列表框中选中“Everyone”账号，只给它赋予“读取”权限；然后单击“添加”按钮，将“System”账号添加到账号列表框中，赋予除“完全控制”和“修改”以外的所有权限，最后单击“确定”按钮，这样当用户清除 Windows 日志时就会弹出错误对话框。

7. 日志分析工具

当网络日志（如 IIS 或 Apache）的数量非常大的时候，人工分析的效率是极低的。这时需要工具来帮忙，Awstats、Faststs Analyzer、Logs2Intrusions v.1.0 等都是很不错的网络日志分析工具。

1.6　网络数据安全

网络中的数据一般可分为三部分：网络数据库中存储的数据、正在传输的数据和在存储介质中存放的数据。大部分数据是存放在网络数据库中的，一小部分数据是在网络中处于正在传输过程中，在存储介质中存放的是小部分临时性的数据。

对这三部分数据，可采取不同的措施和方法保证其安全。对于存储在数据库中的数据可采用数据的备份和恢复等方法保证其安全；对于正在传输过程中的数据，可采取通信加密技术和鉴别技术保证其安全；对于在存储介质中暂时存放的数据可采取硬件介质保护、文件加密和软件措施等保证其安全。

1.6.1　存储介质的数据安全

目前在网络系统中使用的存储介质除传统的磁带、硬盘外，使用较多、较频繁的是移动存储介质。这些移动存储介质包括 U 盘、软盘、光盘、移动硬盘、外挂 IDE 及各类移动存储卡等。这些存储介质具有设备小型化、形式多样化和存储量大的特点。移动存储介质的出现和普及应用，虽然为用户在数据交换和存储过程中提供了极大的方便，但也给这些存储介质管理和文件信息管理带来一定的困难。因为任何个人的 U 盘、移动硬盘、软盘或光盘都可在一般的计算机上随意使用，这就使得病毒防范难度加大，容易形成病毒传播源，造成计算机病毒感染和泛滥；信息易丢失；介质交叉共用，存在泄密隐患；缺少有效的移动设备管理监督机制；单位内部人员可以随意将内部的重要信息复制出去，造成敏感信息泄密；移动存储介质一旦丢失，存储的大量敏感数据可能失控，造成泄密等。

1．存储介质中的数据保护

在使用计算机的过程中，移动存储介质的使用和管理环节存在一些安全隐患，尤其是在维修和报废处理上不遵守保密管理规定，缺乏安全保密意识，给涉密数据带来很大的安全风险。

对于存有大量信息的移动存储介质的管理，应坚持预防为主，规范涉密存储介质处置工作，定期检查涉密系统，从软件上把好安全保密关，加强管理、堵塞管理制度上的安全漏洞，充分利用管理和技术两方面的手段，达到有效防范信息泄密的目的。

（1）强化管理，加强“人防”，健全安全保密的监督机制

① 加强保密知识和职业道德教育，提高员工的综合素质。树立“保密就是保安全、就是保效益”的理念，从思想上筑起一道信息安全防范屏障。

② 要开展安全知识培训，提高安全防范能力。用典型案例教育用户，使他们充分了解移动存储介质在使用中存在的安全隐患，提高工作人员的安全保密意识和自我防范能力。

③ 加强内部管理，防范内部风险。主要是进一步完善存储介质的管理制度，细化各个环节的管理规范和责任追究制度，明确界定涉密信息范围，实现移动存储介质信息安全保密工作的规范化管理。

④ 加强对移动存储介质管理的监督检查。要形成机制，对移动存储介质进行经常检

查。要树立管理权威,任何人用于工作的移动存储介质都要接受检查。如果发现违规情况应依据规章制度进行处理,以警示他人。

⑤ 对现有的各类移动存储介质进行登记造册,明确使用人员的管理使用职责。做到责任到人,未经保密部门登记的移动存储介质严禁存储涉密文件、数据。严禁将移动存储介质转借他人使用。未经技术处理的移动介质不得外送修理、不得擅自销毁移动存储介质。

⑥ 加强对外来人员技术服务的管理。应当进一步规范外来人员技术服务工作,在外来人员进行技术服务时要指派专人监督,以防范外来人员通过技术服务方式窃取涉密信息及重要数据。

⑦ 建立文件备份和定期杀毒制度。对于存储的重要信息要及时进行备份,要对移动存储介质定期杀毒,做好重要信息的防丢失和防损坏工作。

⑧ 可对移动存储介质进行分组管理,支持针对设备组的策略设置。

⑨ 支持移动存储介质使用只读、禁用、加密读写和正常读写等数据处理方式,提供灵活的存储介质控制方法。

⑩ 提供详细的审计记录,包括注册信息、使用信息和文件操作信息,记录要素包括使用人、使用计算机、使用时间和动作等,并提供丰富的审计报告。

(2) 突出“技防”,构筑安全保密的“防火墙”

① 大力投入。树立“花钱买保密,投资保安全”的思想,加大技术防范设备的投资,不断完善技术保密设施。

② 采用加密存储技术。对涉密存储介质进行加密,即使发生介质丢失或失窃事件,也可确保存储介质上的涉密信息不会轻易泄露出去。

③ 建立安全的身份认证机制。这样可有效地防止未经授权的用户使用存储介质获取敏感信息。

④ 对文件加密。对移动存储介质上的文件和文件夹进行加密。经加密处理后,只有那些经过授权的用户才可对加密后的文件和文件夹进行读、写和修改等操作,从而达到保密的目的。通过加密读写策略,还可以有效控制移动存储介质数据的共享范围。

⑤ 防范窃密者非法入侵。通过技术手段使外来移动存储介质无法介入涉密的内部网络,内部网中经过认证后移动存储介质也仅能在授权的客户机上使用。

⑥ 采用存储介质注册机制。这样可使未经注册的移动存储介质不能在受管理的计算机系统中使用;可以设定移动存储介质允许使用的用户(组)和计算机(组);可随时更改移动存储介质的注册策略和信息,包括策略变更、挂失和注销等;对未注册的移动存储介质,可提供默认策略(禁用、只读、加密和正常读写等)的支持,从而降低管理难度。

⑦ 对移动存储介质加入识别信息,并与安全策略配合,即可控制在哪台设备上能使用移动存储介质,哪些用户可以使用这些移动存储介质,使用到何种程度(只读还是读写)等。

⑧ 采用电子证书形式对移动存储介质进行认证管理。这样可做到如果不知道证书的PIN码,就无法读取移动介质中的数据。

⑨ 加强对USB端口进行管理。USB端口和USB存储设备不同,如果禁用USB端口,则所有的USB设备都不能使用,其中包括USB键盘和鼠标。

由于USB端口目前被广泛使用,通过对端口的禁用可直接影响用户的使用,所以对于U盘的管理,应在保证USB端口易用性的同时又能保证U盘的安全使用。目前市面上已

经有相关的产品实现了对 U 盘的认证管理,这样既保证了 USB 口的使用又有效地规范了 U 盘的使用。

2. 存储介质的实体保护

存储介质或其存储信息的丢失,或对它们的非法复制和窃取,都将对网络系统造成不同程度的损失。因此,要对存储介质实体进行保护,可采取如下安全保护措施。

① 建立专门的存储介质库(柜),对存储介质库(柜)的访问要限于少数的管理员和操作员。存储介质库(柜)内磁带、磁盘等介质的目录清单要标明文件名、文件所有者、序列号、项目号、建立日期和保留日期等参数。

② 所有存储介质不用时要放在存储介质库(柜)内。

③ 要保持存储介质库(柜)房内有合适的温度、湿度。

④ 对保管的磁带、磁盘要做定期检查,以防信息丢失。

⑤ 对需要长期保存的有效数据,应在存储介质的质量保证期内进行转储,转储时应确保内容正确。

⑥ 打印有业务数据或程序的纸质介质,要视同档案,妥为保管。

⑦ 旧存储介质销毁前进行消磁和清除数据处理。

1.6.2　网络数据的备份与恢复

在日常工作中,计算机病毒、黑客攻击、人为操作错误、系统软件或应用软件缺陷、硬件损毁、突然断电、意外宕机、自然灾害等诸多因素都有可能造成计算机中数据的丢失,给用户造成无法估量的损失。因此,对重要数据进行备份与恢复对用户来说显得格外重要。

1. 数据备份

(1) 数据备份的概念

数据备份就是指为防止系统出现操作失误或系统故障导致数据丢失,而将全部或部分数据集合从应用主机的硬盘或阵列中复制到其他存储介质上的过程。计算机系统中的数据备份,通常是指将存储在计算机系统中的数据复制到相应的存储介质上,在计算机以外的地方另行保管。这样,当计算机系统设备发生故障或发生其他威胁数据安全的灾害时,能及时地从备份的介质上恢复正确的数据。

数据备份就是为了系统数据崩溃时能够快速地恢复数据,使系统迅速恢复运行。那么就必须保证备份数据和源数据的一致性和完整性,消除系统使用者的后顾之忧。其关键在于保障系统的高可用性,即操作失误或系统故障发生后,能够保障系统的正常运行。如果没有了数据,一切恢复都是不可能实现的,因此备份是一切灾难恢复的基石。从这个意义上说,任何灾难恢复系统实际上都是建立在备份基础上的。数据备份与恢复系统是数据保护措施中最直接、最有效、最经济的方案,也是任何计算机信息系统不可缺少的一部分。

现在不少用户也意识到了这一点,采取了系统定期检测与维护、双机热备份、磁盘镜像或容错、备份磁带异地存放、关键部件冗余等多种预防措施。这些措施一般能够进行数据备份,并且在系统发生故障后能够进行快速系统恢复。

数据备份能够用一种增加数据存储代价的方法保护数据安全,它对于拥有重要数据的

大企事业单位是非常重要的,因此数据备份和恢复通常是大中型企事业网络系统管理员每天必做的工作之一。对于个人计算机用户,数据备份也是非常必要的。

传统的数据备份主要是采用内置或外置的磁带机进行冷备份。一般来说,各种操作系统都附带了备份程序。但随着数据的不断增加和系统要求的不断提高,附带的备份程序已无法满足需求。要想对数据进行可靠的备份,必须选择专门的备份软、硬件,并制定相应的备份及恢复方案。

目前比较常用的数据备份工具如下。

① 本地磁带备份。利用大容量磁带备份数据。

② 本地可移动存储器备份。利用大容量等价软盘驱动器、可移动等价硬盘驱动器、一次性可刻录光盘驱动器、可重复刻录光盘驱动器进行数据备份。

③ 本地可移动硬盘备份。利用可移动硬盘备份数据。

④ 本机多硬盘备份。在本机内装有多块硬盘,利用除安装和运行操作系统和应用程序的硬盘外的其余硬盘进行数据备份。

⑤ 远程磁带库光盘库备份。将数据传送到远程备份中心制作完整的备份磁带或光盘。

⑥ 远程数据库备份。在与主数据库所在生产机相分离的备份机上建立主数据库的一个复制。

⑦ 网络数据镜像。对生产系统的数据库数据和所需跟踪的重要目标文件的更新进行监控与跟踪,并将更新日志实时通过网络传送到备份系统,备份系统则根据日志对磁盘进行更新。

⑧ 远程镜像磁盘。通过高速光纤通道线路和磁盘控制技术将镜像磁盘延伸到远离生产机的地方,镜像磁盘数据与主磁盘数据完全一致,更新方式为同步或异步。

(2) 数据备份的类型

按数据备份时数据库状态的不同可分为冷备份、热备份和逻辑备份等数据备份类型。

① 冷备份

冷备份(cold backup)是指在关闭数据库的状态下进行的数据库完全备份。备份内容包括所有的数据文件、控制文件、联机日志文件等。因此,在进行冷备份时数据库不能被访问。冷备份通常只采用完全备份。

② 热备份

热备份(hot backup)是指在数据库运行状态下对数据文件和控制文件进行的备份。使用热备份必须将数据库运行在归档方式下。在进行热备份的同时可以进行数据库的各种操作。

③ 逻辑备份

逻辑备份是最简单的备份方法,可按数据库中某个表、某个用户或整个数据库进行导出。使用这种方法时数据库必须处于打开状态,且如果数据库不是在 restrict 状态将不能保证导出数据的一致性。

(3) 数据备份策略

需要进行数据备份的部门都要先制定数据备份策略。数据备份策略包括确定需备份的数据内容(如进行完全备份、增量备份、差别备份还是按需备份)、备份类型(如采用冷备份还是热备份)、备份周期(如以月、周、日还是小时为备份周期)、备份方式(如采用手工备份还是

自动备份）、备份介质（如以光盘、硬盘、磁带还是 U 盘做备份介质）和备份介质的存放等。下面是不同数据内容的几种备份方式。

① 完全备份

完全备份（full backup）是指按备份周期（如一天）对整个系统所有的文件（数据）进行备份。这种备份方式比较流行，也是克服系统数据不安全的最简单方法，操作起来比较方便。有了完全备份，可恢复网络系统备份日之前的所有信息，恢复操作也可一次性完成。如当发现数据丢失时，只要用一盘故障发生前一天备份的磁带，即可恢复丢失的数据。但这种方式的不足之处是由于每天都对系统进行完全备份，在备份数据中必定有大量的内容是重复的，这些重复的数据占用了大量的磁带空间，这对用户来说就意味着增加成本；另外，由于进行完全备份时需要备份的数据量相当大，因此备份所需时间较长。对于那些业务繁忙，备份窗口时间有限的单位，选择这种备份策略是不合适的。

② 增量备份

增量备份（incremental backup）是指每次备份的数据只是相当于上一次备份后增加和修改过的内容，即备份的都是已更新过的数据。比如，系统在星期日做了一次完全备份，然后在以后的六天里每天只对当天新的或被修改过的数据进行备份。这种备份的优点是没有或减少了重复的备份数据，既节省存储介质空间，又缩短了备份时间。但它的缺点是恢复数据过程比较麻烦，不可能一次性地完成整体的恢复。

③ 差别备份

差别备份（differential backup）也是在完全备份后将新增加或修改过的数据进行备份，但它与增量备份的区别是每次备份都把上次完全备份后更新过的数据进行备份。比如，星期日进行完全备份后，其余六天中的每一天都将当天所有与星期日完全备份时不同的数据进行备份。差别备份可节省备份时间和存储介质空间，只需两盘磁带（星期日备份磁带和故障发生前一天的备份磁带）即可恢复数据。差别备份兼具了完全备份的发生数据丢失时恢复数据较方便和增量备份的节省存储空间及备份时间的优点。

完全备份所需的时间最长，占用存储介质容量最大，但数据恢复时间最短，操作最方便，当系统数据量不大时该备份方式最可靠；但当数据量增大时，很难每天都做完全备份，可选择周末做完全备份，在其他时间采用所用时间最少的增量备份或时间介于两者之间的差别备份。在实际备份中，通常也是根据具体情况，采用这几种备份方式的组合，如年底做完全备份，月底做完全备份，周末做完全备份，而每天做增量备份或差别备份。

④ 按需备份

除以上备份方式外，还可采用对随时所需数据进行备份的方式进行数据备份。按需备份就是指除正常备份外，额外进行的备份操作。额外备份可以有许多理由，比如，只想备份很少几个文件或目录，备份服务器上所有的必需信息，以便进行更安全的升级等。这样的备份在实际应用中经常遇到。

2. 数据恢复

数据恢复是指将备份到存储介质上的数据再恢复到计算机系统中，它与数据备份是一个相反的过程。

数据恢复措施在整个数据安全保护中占有相当重要的地位，因为它关系到系统在经历

灾难后能否迅速恢复运行。

通常，当硬盘数据被破坏时，当需要查询以往年份的历史数据，而这些数据又已从现系统上清除，或当系统需要从一台计算机转移到另一台计算机上运行时，应使用数据恢复功能进行数据恢复。

(1) 恢复数据时的注意事项

- 由于恢复数据是覆盖性的，不正确的恢复可能破坏硬盘中的最新数据，因此在进行数据恢复时，应先将硬盘数据备份。
- 进行恢复操作时，用户应指明恢复何年何月的数据。当开始恢复数据时，系统首先识别备份介质上标识的备份日期是否与用户选择的日期相同，如果不同将提醒用户更换备份介质。
- 由于数据恢复工作比较重要，容易错把系统上的最新数据变成备份盘上的旧数据，因此应指定少数人进行此项操作。
- 不要在恢复过程中关机、关电源或重新启动计算机。
- 不要在恢复过程中打开驱动器开关或抽出软盘、光盘(除非系统提示换盘)。

(2) 数据恢复的类型

一般来说，数据恢复操作比数据备份操作更容易出问题。数据备份只是将信息从磁盘复制出来，而数据恢复则要在目标系统上创建文件。在创建文件时会出现许多差错，如超过容量限制、权限问题和文件覆盖错误等。数据备份操作不需知道太多的系统信息，只需复制指定信息就可以了；而数据恢复操作则需要知道哪些文件需要恢复，哪些文件不需要恢复等。

数据恢复操作通常有全盘恢复、个别文件恢复和重定向恢复三种类型。

① 全盘恢复

全盘恢复就是将备份到介质上的指定系统信息全部转储到它们原来的地方。全盘恢复一般应用在服务器发生意外灾难时导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等，也称为系统恢复。

② 个别文件恢复

个别文件恢复就是将个别已备份的最新版文件恢复到原来的地方。对大多数备份来说，这是一种相对简单的操作。个别文件恢复要比全盘恢复用得更普遍。利用网络备份系统的恢复功能，很容易恢复受损的个别文件。需要时只要浏览备份数据库或目录，找到该文件，启动恢复功能，系统将自动驱动存储设备，加载相应的存储媒体，恢复指定文件。

③ 重定向恢复

重定向恢复是将备份的文件(数据)恢复到另一个不同的位置或系统上去，而不是做备份操作时它们所在的位置。重定向恢复可以是整个系统恢复，也可以是个别文件恢复。重定向恢复时需要慎重考虑，要确保系统或文件恢复后的可用性。

习题和思考题

一、问答题

1. 何为计算机网络安全？网络安全有哪几个特征？其特征的含义是什么？
2. 简述网络安全的需求与目标。

3. 简述 Internet 上的主要危险。

4. 网络系统的脆弱性主要表现在哪几个方面?

5. 网络安全的威胁主要来自哪些方面? 通常说的网络威胁有哪两大类?

6. 简述网络系统的日常管理和安全维护措施。

7. 请列出你熟悉的几种常用的网络安全防护措施。

二、填空题

1. 网络系统的(　　)性是指保证网络系统不因各种因素的影响而中断正常工作。

2. 数据的(　　)性是指在保证软件和数据完整性的同时,还要能使其被正常利用和操作。

3. 网络攻击主要有(　　)攻击和(　　)攻击两大类。

4. 网络威胁主要来自人为影响和外部(　　)的影响,它们包括对网络设备的威胁和对(　　)的威胁。

5. 被动攻击的特点是偷听或监视传送,其目的是获得(　　)。

6. 某些人或某些组织想方设法利用网络系统来获取相应领域的敏感信息,这种威胁属于(　　)威胁。

7. 软、硬件的机能失常、人为误操作、管理不善而引起的威胁属于(　　)威胁。

8. 使用特殊技术对系统进行攻击,以便得到有针对性的信息就是一种(　　)攻击。

9. 数据恢复操作的种类有(　　)、(　　)和重定向恢复。

三、单项选择题

1. 入侵者通过观察网络线路上的信息,而不干扰信息的正常流动,如搭线窃听或非授权地阅读信息,这是属于(　　)。

A. 被动攻击　B. 主动攻击　C. 无意威胁　D. 系统缺陷

2. 入侵者对传输中的信息或存储的信息进行各种非法处理,如有选择地更改、插入、延迟、删除或复制这些信息,这是属于(　　)。

A. 无意威胁　B. 主动攻击　C. 系统缺陷　D. 漏洞威胁

3. 入侵者利用操作系统存在的后门进入系统进行非法操作,这样的威胁属于(　　)。

A. 被动攻击　B. 无意威胁　C. 系统缺陷　D. 窃取威胁

4. 软件错误、文件损坏、数据交换错误、操作系统错误等是影响数据完整性的(　　)原因。

A. 人为因素　B. 软件和数据故障　C. 硬件故障　D. 网络故障

5. 磁盘故障、I/O 控制器故障、电源故障、存储器故障、芯片和主板故障是影响数据完整性的(　　)原因。

A. 人为因素　B. 软件故障　C. 网络故障　D. 硬件故障

6. 属于通信系统与通信协议的脆弱性的是(　　)。

A. 介质的剩磁效应　B. 硬件和软件故障

C. TCP/IP 漏洞　D. 数据库分级管理

7. 属于计算机系统本身的脆弱性的是(　　)。

A. 硬件和软件故障　B. 介质的剩磁效应

C. TCP/IP 漏洞　D. 数据库分级管理

8. 网络系统面临的威胁主要是来自(1)(　　)影响,这些威胁大致可分为(2)(　　)两大类。

(1) A. 无意威胁和故意威胁　　B. 人为和自然环境
　　C. 主动攻击和被动攻击　　D. 软件系统和硬件系统

(2) A. 无意威胁和故意威胁　　B. 人为和自然环境
　　C. 主动攻击和被动攻击　　D. 软件系统和硬件系统

9. 网络安全包括(1)(　　)安全运行和(2)(　　)安全保护两方面的内容。这就是通常所说可靠性、保密性、完整性和可用性。(3)(　　)是指保护网络系统中存储和传输的数据不被非法操作。(4)(　　)是指在保证数据完整性的同时,还要能使其被正常利用和操作。(5)(　　)主要是利用密码技术对数据进行加密处理,保证在系统中传输的数据不被无关人员识别。

(1) A. 系统　　B. 通信　　C. 信息　　D. 传输

(2) A. 系统　　B. 通信　　C. 信息　　D. 传输

(3) A. 保密性　　B. 完整性　　C. 可靠性　　D. 可用性

(4) A. 保密性　　B. 完整性　　C. 可靠性　　D. 可用性

(5) A. 保密性　　B. 完整性　　C. 可靠性　　D. 可用性

第2章 网络设备的安全与应用实践

计算机网络系统的硬件设备一般价格比较昂贵，一旦被破坏且又不能及时修复时，不仅会造成经济损失，而且可能使整个网络系统瘫痪，产生严重的后果。因此必须加强对计算机网络系统硬件设备的使用管理，坚持做好硬件设备的日常维护和保养工作。

对硬件设备的使用管理，通常要做到：

- 根据硬件设备的具体配置，制定切实可行的硬件设备操作使用规范，并严格按照规范进行操作。
- 建立设备使用情况日志，并严格登记使用过程情况。
- 建立硬件设备故障情况登记表，详细记录故障性质和修复情况。
- 坚持对硬件设备进行例行维护和保养，并指定专人负责。

对硬件设备的维护和保养，就是要对常用的硬件设备进行必要的维护和保养，这些硬件设备包括客户端硬件设备(如主机、显示器、软驱、打印机、硬盘)和网络设备(如 Hub、交换机、路由器、Modem、RJ-45 接头、网络线缆、各种服务器)。此外，还要定期检查供电系统的各种保护装置及地线是否正常。

2.1 物理安全

计算机系统无论是硬件还是软件都不可避免存在发生故障的可能，但并不是发生故障就一定意味着该系统完全失效。计算机系统大多拥有“容错”能力，即允许存在某些错误，尽管系统硬件有故障或程序有错误，仍能正确执行特定算法和提供系统服务。

2.1.1 网络的冗余安全

采用“冗余技术”是实现计算机容错的主要手段。“冗余”就是增加一些多余设备，以保证系统更加可靠、安全地工作。冗余的分类方法多种多样，按照在系统中所处的位置，冗余可分为元件级、部件级和系统级；按照冗余的程度可分为 1∶1 冗余、1∶2 冗余、1∶n 冗余等。在当前元器件可靠性不断提高的情况下，与其他形式的冗余方式相比，1∶1 的部件级热冗余是一种有效而又相对简单、配置灵活的冗余技术实现方式，如 I/O 卡件冗余、电源冗余、主控制器冗余等。

冗余设计的目的是：系统运行不受局部故障的影响，故障部件的维护对整个系统的功能实现没有影响，并可以实现在线维护，使故障部件得到及时的修复。冗余设计会增加系统

设计的难度,冗余配置会增加用户的投资,但这种投资换来了系统的可靠性,提高了整个用户系统的平均无故障时间,缩短了平均故障修复时间。两个部件组成的并联系统(互为冗余)与单部件相比,平均无故障时间是原来的1.5倍。系统的可用性指标可以用两个参数进行简单的描述:一个是平均无故障时间(MTBF),MTBF一般指产品在两次故障之间的平均时间间隔,是产品的平均寿命的指标之一;另一个是平均修复时间(MTBR),MTBR一般指产品的故障维修所需的平均修复时间,是产品可维修性的衡量指标,MTBR越短表示易恢复性越好。

1. 网络拓扑设计的冗余链路

在企业进行网络拓扑结构的设计时,一般采取星型结构和环型结构的混合。在核心层采用环型结构,在汇聚层和接入层采取星型结构,并充分考虑双核心交换机和汇聚交换机以及网络服务设备之间在物理链路上的冗余。正常工作时,冗余的两条数据高速通路同时并行工作,自动分摊网络流量,使系统网络通信带宽提高。当其中一路故障(接口损坏或出现线路故障)时,另一路自动地承担全部通信负载,保证通信的正常进行,如图2.1所示。

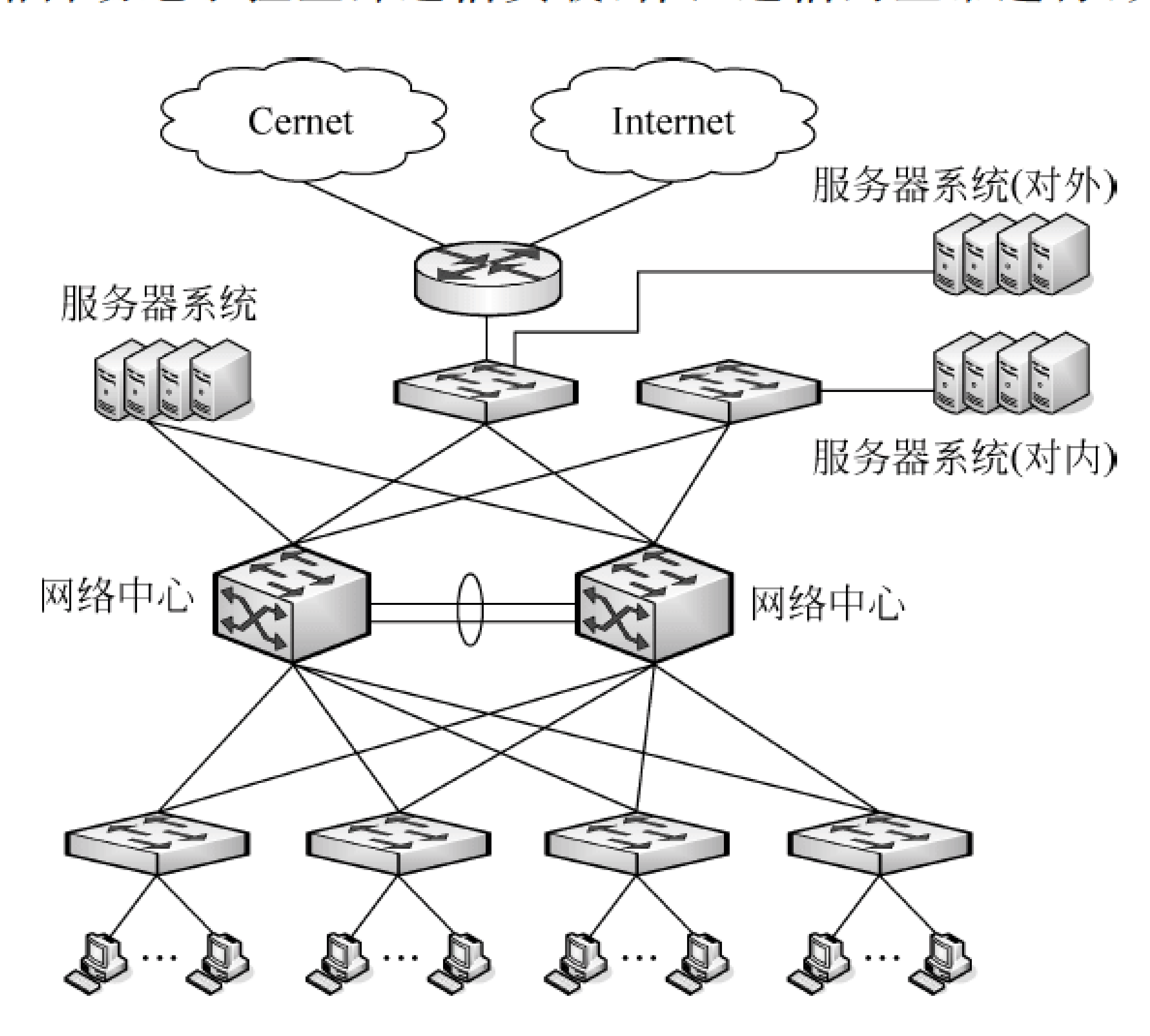


图2.1 网络拓扑设计中实现链路的冗余

2. 供电系统的冗余

电源是整个网络系统得以正常工作的动力源泉。一旦电源单元发生故障,往往会使整个系统的工作中断,造成严重后果。要使系统能够安全可靠、长期、稳定地运行,首先必须保证稳定供电。供配电系统的安全、可靠是保证机房设备安全可靠运行的关键。机房设备属于一级负荷,按一级负荷的供电要求必须保证两个以上独立的电源点供电。

采用冗余的电源备份方案,并保障充分、持续的电力供应。对于城市供电而言相对比较稳定,一般不会长时间停电,如果停电也将是区域性停电,因此可考虑使用UPS作为备份电源。电池延时时间的长度要根据机房的实际情况来定,一般建议一小时以上。结合实际情况,采用市电+UPS后备电池相结合的供电方式。正常情况下,市电通过UPS稳频稳压后,给计算机设备供电,保证计算机设备的电能质量。当市电停电时,后备电池通过UPS逆

变后，给计算机设备供电。市电与 UPS 后备电池间通过静态转换开关切换，确保计算机设备无瞬间断电。

2.1.2　网络设备的冗余

网络系统的主要设备有核心交换机、服务器、存储设备以及网络边界设备（如路由器、防火墙）等。为保证网络系统能正常运行和提供正常的服务，在进行网络设计时要充分考虑主要设备的部件或设备的冗余。

1. 核心交换机冗余

核心交换机在网络运行和服务中占有非常重要的地位，在冗余设计时要充分考虑该设备的部件和设备的冗余，以保证网络的可靠性。

核心交换机中电源模块的故障率相对较高，为了保证核心交换机的正常运行，一般考虑在核心交换机上增配一块电源模块，实现该部件的冗余。为了保证核心交换机的可靠运行，可在本地机房配备双核心交换机或在异地配备双核心交换机，通过链路的冗余实行核心交换设备的冗余。同时针对网络的应用和扩展需要，还需在网络的各类光电接口以及插槽数上考虑有充分的冗余。

2. 服务器冗余

在网络系统中，服务器的种类和应用比较多，冗余设计是非常必要的。如数千台计算机的 IP 地址管理是个大问题，为了解决这个问题，许多企业网络会采用 DHCP 服务器来动态地给客户机分配 IP 地址。但是这同样潜在一种安全隐患，即如果 DHCP 服务器因为某种原因瘫痪了，DHCP 服务自然也就无法使用，客户机也就无法获得正确的 IP 地址，从而影响整个企业网络的正常运行。

可以通过同时配置两台 DHCP 服务器来解决该问题。如果其中的一台 DHCP 服务器有故障了，另一台 DHCP 服务器就会自动承担分配 IP 地址的任务。对于用户来说，这个过程是透明的，用户并不知道 DHCP 服务器的变化。

为了保证系统的可靠性，通常对服务器还可采用部件冗余技术、RAID 技术等为计算机的日常工作保驾护航。

（1）部件冗余技术

服务器是由众多部件模块组成的，通常情况下，故障会在一些特定的模块发生（如电源），为此服务器也可采用特定模块冗余，如配备双电源。这样，当一个电源发生故障停止运转，另一个电源仍然能够提供服务器正常运转所需要的能源。

（2）RAID 技术

廉价冗余磁盘阵列（redundant array of independent disks，RAID）技术就是利用多个磁盘的组合提供高效率及冗余的功能。采用 RAID 技术可保护硬盘中的数据不因硬盘的物理损坏而丢失。RAID 技术有多个级别，目前常用的 RAID 级别有 RAID0、RAID1 和 RAID5 等。

3. 存储设备冗余

存储设备是数据存储的载体。为了保证存储设备的可靠性和有效性可在本地或异地设

计存储设备冗余。目前数据的存储设备多种多样，根据需要可选择刻录光驱、磁带机、磁盘阵列等设备冗余。

4. 网络边界设备冗余

对于比较重要的网络系统或重要的服务系统，对路由器和防火墙等网络边界设备的可用性要求也非常高，一旦该类设备出现故障则影响内网和外网的互连。因此，在必要的时候可对部分网络边界设备进行冗余设计。

2.2 路由器安全与应用实践

路由器是网络的神经中枢，是众多网络设备的重要一员，它担负着网间互连、路由走向、协议配置和网络安全等重任，是信息出入网络的必经之路。广域网就是靠一个个路由器连接起来组成的，局域网中也已经普遍应用到了路由器。在很多企事业单位，已经用路由器来接入网络进行数据通信，可以说，路由器现在已经成为大众化的网络设备了。

路由器对网络的应用和安全具有极重要的地位。随着路由器应用的广泛和普及，它的安全性也成为一个热门话题。路由器的安全直接关系到网络的安全。下面介绍网络安全中路由器的安全配置。

2.2.1 路由协议与访问控制

1. 路由选择及协议

路由器是网络互连关键设备，其主要工作是为经过路由器的多个分组寻找一个最佳传输路径，并将分组有效地传输到目的地。路由选择是根据一定的原则和算法在多节点的通信子网中选择一条从源节点到目的节点的最佳路径。当然，最佳路径是相对于几条路径中较好的路径而言的，一般是选择时延小、路径短、中间节点少的路径作为最佳路径。通过路由选择，可使网络中的信息流量合理分配，减轻拥挤，提高传输效率。

路由选择算法可分为静态路由选择算法和动态路由选择算法两大类。静态路由选择是根据某种固定的规则进行的，路由选择一旦完成就不再变化，不会对网络的信息流量和拓扑变化作出响应，因此也称为非自适应性路由选择算法；动态路由选择是根据网络拓扑结构和信息流量的变化而改变的路由选择，因此也称为自适应性路由选择算法。

在路由器上利用路由选择协议主动交换路由信息，建立路由表并根据路由表转发分组。通过路由选择协议，路由器可动态适应网络结构的变化，并找到到达目的网络的最佳路径。路由表可以是事先设置好的(称为静态路由表)，一旦它固定下来，就不会随将来网络结构和状态的变化而变化；路由表也可以是由系统动态修改的(称为动态路由表)，利用路由器的自学习能力自动记忆网络的运行情况，计算出最佳传输路径，当网络的外部条件改变时，路由器能重新自学习并动态修改路由表，保证网络传输的实效性。动态路由表可以由路由器自动调整，也可以由主机控制调整。

静态路由算法在网络业务量或拓扑结构变化不大的情况下，才能获得较好的网络性能。在现代网络中，广泛采用的是动态路由算法。在动态路由选择算法中，分布式路由选择算法

是很优秀的，得到了广泛的应用。在该类算法中，最常用的是距离向量路由选择(distance vector routing，DVR)算法和链路状态路由选择(link state routing，LSR)算法。前者经过改进，成为目前广泛应用的路由信息协议(routing information protocol，RIP)，后者则发展成为开放式最短路径优先(open shortest path first，OSPF)协议。

2. 路由器访问控制列表(ACL)

ACL 是 Cisco IOS 所提供的一种访问控制技术，初期仅在路由器上应用，近些年来已经扩展到三层交换机，部分最新的二层交换机(如 2950)也开始提供 ACL 支持。在其他厂商的路由器或多层交换机上也提供类似技术，但名称和配置方式可能有细微的差别。

ACL 技术在路由器中被广泛采用，它是一种基于包过滤的流控制技术。ACL 在路由器上读取第三层及第四层包头中的信息(如源地址、目的地址、源端口、目的端口等)，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。ACL 增加了在路由器接口上过滤数据包出入的灵活性，可以帮助管理员限制网络流量，也可以控制用户和设备对网络的使用。它根据网络中每个数据包所包含的信息内容决定是否允许该信息包通过接口。

ACL 有标准 ACL 和扩展 ACL 两种。标准 ACL 把源地址、目的地址及端口号作为数据包检查的基本元素，并规定符合条件的数据包是否允许通过，其使用的局限性大，其序列号范围是 1～99。扩展 ACL 能够检查可被路由的数据包的源地址和目的地址，同时还可以检查指定的协议、端口号和其他参数，具有配置灵活、精确控制的特点，其序列号范围是 100～199。

这两种类型的 ACL 都可以基于序列号和命名进行配置。最好使用命名方法配置 ACL，这样对以后的修改是很方便的。配置 ACL 要注意两点：一是 ACL 只能过滤流经路由器的流量，对路由器自身发出的数据包不起作用；二是一个 ACL 中至少有一条允许语句。

ACL 的主要作用就是一方面保护网络资源，阻止非法用户对资源的访问；另一方面限制特定用户所能具备的访问权限。它通常应用在企业内部网的出口控制上，通过实施 ACL，可以有效地部署企业内部网的出口策略。随着企业内部网资源的增加，一些企业已开始使用 ACL 控制对企业内部网资源的访问，进而保障这些资源的安全性。

2.2.2　虚拟路由器冗余协议

1. VRRP 协议

在建立一个网络时，为了保证网络稳定可靠地运行，经常采用一些动态路由协议，如 OSPF、RIP 等。这些路由协议可以自动绕开很多网络故障(如路由器 Down 机)，但很多时候可能无法使用这些高端的路由协议。比如，用户端要配置 OSPF、RIP 协议必须有上游 ISP 供应商的支持，但很多 ISP 供应商是不提供这种服务的，他们只提供静态路由。虚拟路由器冗余协议(virtual router redundancy protocol，VRRP)可以完成这些工作。

VRRP 是一种选择协议，它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中。使用 VRRP，可以通过手动或 DHCP 设定一个虚拟 IP 地址作为默认路由器。虚拟 IP 地址在路由器间共享，控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由

器，其他的则为备份路由器。主路由器负责转发数据包到这些虚拟 IP 地址。如果主路由器不可用，这个虚拟 IP 地址就会映射到一个备份路由器的 IP 地址(该备份路由器就成为主路由器)。使用 VRRP 的好处是有更高的默认路径的可用性而无须在每个终端主机上配置动态路由或路由发现协议。另外，如果用户端有两条以上的 Internet 线路，VRRP 也可对它们进行负载均衡和路由器备份。为了保证网络的不间断、稳定的运行，VRRP 是一个最好的选择。VRRP 是 IPv4 和 IPv6 的一部分。

VRRP 是一种容错协议，它为具有多播或广播能力的局域网(如以太网)而设计。VRRP 将局域网的一组路由器(包括一个主路由器和若干个备份路由器)组织成一个虚拟路由器，称为一个备份组。

这个虚拟路由器拥有自己的 IP 地址 10.100.10.1，备份组内的路由器也有自己的 IP 地址(如 Master 的 IP 地址为 10.100.10.2，Backup 的 IP 地址为 10.100.10.3)。局域网内的主机仅仅知道这个虚拟路由器的 IP 地址 10.100.10.1，而并不知道具体的 Master 路由器的 IP 地址 10.100.10.2 以及 Backup 路由器的 IP 地址 10.100.10.3，它们将自己的默认路由下一跳地址设置为该虚拟路由器的 IP 地址 10.100.10.1。于是，网络内的主机就通过这个虚拟的路由器来与其他网络进行通信。如果备份组内的 Master 路由器坏掉，Backup 路由器将会通过选举策略成为一个新的主路由器，继续向网络内的主机提供路由服务，从而实现网络内的主机不间断地与外部网络进行通信。

在 VRRP 路由器组中，按优先级选举主路由器，VRRP 协议中优先级范围是 0～255。若 VRRP 路由器的 IP 地址和虚拟路由器的接口 IP 地址相同，则把该虚拟路由器称作 VRRP 组中的 IP 地址所有者；IP 地址所有者自动具有最高优先级 255。优先级 0 一般在 IP 地址所有者主动放弃主控者角色时使用。可配置的优先级范围为 1～254。因此，如果在 VRRP 组中有 IP 地址所有者，则它总是作为主控路由的角色出现。

为了保证 VRRP 协议的安全性，提供了明文认证和 IP 头认证两种安全认证措施。明文认证方式要求在加入一个 VRRP 路由器组时，必须同时提供相同的 VRID 和明文密码。IP 头认证方式提供了更高的安全性，能够防止报文重放和修改等攻击。

2. Linux 下的 VRRP 组件

在 Linux 操作系统下可以实现非常稳定的 VRRP 功能，实现该功能的软件是 Keepalived。Keepalived 起初是为 LVS(Linux Virtual Server，Linux 下的服务器负载均衡系统)设计的，专门用来监控服务器的状态，后来加入了 VRRP 的功能。Keepalived 的 VRRP 功能是从 Linux 中 VRRPD 发展而来的。

3. Keepalived 的安装

安装 Keepalived 需要先安装 openssl 和 popt 两个组件。

(1) openssl 的安装

如果系统已经有了 openssl，且在/usr/include 目录下有 openssl 的目录，那么 openssl 就不需要安装了，否则需要安装。

```
tar zxvf openssl-0.9.7d.tar.gz
cd openssl-0.9.7d
```

```
configure
make
make test
make install
```

openssl 安装后，再将其 include 目录复制到/usr/include：

```
cp －r /usr/local/ssl/include/openssl /usr/include(T115)
```

（2）popt 的安装

```
tar zxvf popt－1.7.tar.gz
cd popt－1.7
./configure
Make
make install
```

（3）编译 Linux 内核

在安装 Keepalived 之前，还需要重新编译 Linux 的内核。将 Netlink、Linux Virtual Server 和组播功能的选项编译进新内核，如图 2.2 所示。

```
Networking options
<*> Packet socket
[*]   Packet socket: mmapped IO
<*> Netlink device emulation
[*] Network packet filtering (replaces ipchains)
[*]   Network packet filtering debugging (NEW)
[*] Socket Filtering
<*> Unix domain sockets
[*] TCP/IP networking
[*]   IP: multicasting
[*]   IP: advanced router
[*]     IP: policy routing (NEW)
[*]       IP: use netfilter MARK value as routing key (NEW)
[*]       IP: fast network address translation (NEW)
[*]     IP: equal cost multipath (NEW)
[*]     IP: use TOS value as routing key (NEW)
[*]     IP: verbose route monitoring (NEW)
[ ]   IP: kernel level autoconfiguration
<*>   IP: tunneling
<*>   IP: GRE tunnels over IP
[*]     IP: broadcast GRE over IP (NEW)
[*]   IP: multicast routing
[*]     IP: PIM-SM version 1 support (NEW)
[*]     IP: PIM-SM version 2 support (NEW)
[*]   IP: TCP Explicit Congestion Notification support
[*]   IP: TCP syncookie support (disabled per default)
  IP: Netfilter Configuration  --->
  IP: Virtual Server Configuration  --->
<*> 802.1Q VLAN Support
```

```
IP: Virtual Server Configuration
<*> virtual server support (EXPERIMENTAL) (NEW)
[*]   IP virtual server debugging (NEW)
(12)   IPVS connection table size (the Nth power of 2) (NEW)
--- IPVS scheduler
<*>   round-robin scheduling (NEW)
<*>   weighted round-robin scheduling (NEW)
<*>   least-connection scheduling scheduling (NEW)
<*>   weighted least-connection scheduling (NEW)
<*>   locality-based least-connection scheduling (NEW)
<*>   locality-based least-connection with replication scheduling (NEW)
<*>   destination hashing scheduling (NEW)
<*>   source hashing scheduling (NEW)
<*>   shortest expected delay scheduling (NEW)
<*>   never queue scheduling (NEW)
--- IPVS application helper
<*>   FTP protocol helper (NEW)
```

图 2.2　Keepalived 的安装

(4) 安装 Keepalived

```
tar zxvf keepalived-1.1.7.tar.gz
cd keepalived-1.1.7
./configure -prefix=/usr/local/keepalived
Make
make install
```

通过 Keepalived 在 Linux 操作系统的安装,就可以实现稳定的 VRRP 功能。

2.2.3 路由器安全配置与应用实践

1. 路由器的自身安全

(1) 用户口令安全

路由器有普通用户和特权用户之分,口令级别有十多种。如果使用明码在浏览或修改配置时容易被其他无关人员窥视到。可在全局配置模式下使用命令

```
service password-encryption
```

进行配置,该命令可将明文密码变为密文密码,保证用户口令的安全。该命令具有不可逆性,即它可将明文密码变为密文密码,但不能将密文密码变为明文密码。

(2) 配置登录安全

路由器的配置一般有控制口(console)配置、Telnet 配置和 SNMP 配置 3 种方法。控制口配置主要用于初始配置,使用中英文终端或 Windows 的超级终端;Telnet 配置方法一般用于远程配置,但由于 Telnet 是明文传输的,很可能被非法窃听而泄露路由器的特权密码,影响安全;SNMP 的配置则比较麻烦,故使用较少。

为了保证使用 Telnet 配置路由器的安全,网络管理员可以采用相应技术措施,仅让路由器管理员的工作站登录而不让其他机器登录到路由器,以保证路由器配置的安全。

使用 IP 标准访问列表控制语句,在 Cisco 路由器的全局配置模式下输入:

```
#access-list 20 permit host 192.120.12.20
```

该命令表示只允许 IP 为 192.120.12.20 的主机登录到路由器。为了保证 192.120.12.20 这一 IP 地址不被其他机器假冒,可以在全局配置模式下输入:

```
#arp 192.120.12.20 xxxx.xxxx.xxxx arpa
```

该命令可把该 IP 地址与其网卡物理地址绑定,xxxx.xxxx.xxxx 为机器的网卡物理地址。这样就可以保证在用 Telnet 配置路由器时不会泄露路由器的口令。

2. 路由器访问控制的安全策略

在利用路由器进行访问控制时可考虑如下安全策略。

(1) 严格控制可以访问路由器的管理员。对路由器的任何一次维护都需要记录备案,要有完备的路由器的安全访问和维护记录日志。

(2) 建议不要远程访问路由器。即使需要远程访问路由器,应使用访问控制列表和高

强度的密码控制。

(3) 要严格地为 IOS(Cisco 网际操作系统)作安全备份,及时升级和修补 IOS 软件,并迅速为 IOS 安装补丁。

(4) 要为路由器的配置文件作安全备份。

(5) 为路由器配备 UPS 设备,或者至少要有冗余电源。

(6) 为进入特权模式设置强壮的密码,可采用 enable secret(不要采用 enable password)命令进行设置,并且启用 Service password-encryption,操作如下:

```
Router(config)#service password-encryption
Router(config)#enable secret
```

(7) 严格控制 CON 端口的访问。具体的措施如下。

① 打开机箱,切断与 CON 口互连的物理线路。

② 改变默认的连接属性,例如修改波特率(默认是 96 000,可以改为其他值)。

③ 给 CON 口设置高强度的密码。

④ 配合使用 ACL 控制对 CON 口的访问,可进行如下操作。

```
Router(Config)#Access-list 1 permit 192.168.0.1
Router(Config)#line con 0
Router(Config-line)#Transport input none
Router(Config-line)#Login local
Router(Config-line)#Exec-timeout 5 0
Router(Config-line)#access-class 1 in
Router(Config-line)#end
```

(8) 如果不使用 AUX 端口,则应禁止该端口,使用如下命令即可(默认情况下是未被启用)。

```
Router(config)#line aux 0
Router(config-line)#transport input none
Router(config-line)#no exec
```

(9) 若要对权限进行分级,采用权限分级策略,可进行如下操作。

```
Router(Config)#username test privilege 10 xxxx
Router(Config)#privilege EXEC level 10 telnet
Router(Config)#privilege EXEC level 10 show ip access-list
```

3. 路由协议的安全配置

只有保证路由协议的有效性和正确性,路由器才能正常工作。比较常用的路由协议有距离向量协议 RIP、开放式最短路径优先协议 OSPF 和增强内部网关选择协议 EIGRP (enhancd interior gateway routing protocol)。为保证路由协议的正常运行,网络管理员在配置路由器时要使用协议认证。认证和具体操作如下。

(1) RIP 路由协议验证

假设串行口 Serial 1 运行 RIP 协议,并且需要 RIP 验证。那么在全局配置模式下输入:

```
# key chain rip-test(rip-test 是关键链名)
# key 1
# key-string password (password 是认证字符串,任取)
# router rip validate-update-source
# inter serial 1
# ip rip authentication key-chain rip-testip rip authentication mode md5
```

要说明的是,在所运行 RIP 协议的接口上才需要进行验证,并且运行 RIP 协议双方的路由器都要有相同的配置,否则 RIP 路由信息不能够很好地交换。

(2) OSPF 路由协议验证

OSPF 有三种认证方法,简单口令认证、MD5 认证和 Null 认证。在默认时 OSPF 使用 Null 认证,也就是路由交换不通过认证。

① 简单口令认证。

在全局配置模式下输入:

```
# ip ospf authentication-key 0 password
# router ospf 100
# area 0.0.0.0 authentication
```

② MD5 认证。

在全局配置模式下输入:

```
# ip ospf message-digest-key 10 md5 password
# router ospf 100
# area 0 authentication message-digest
```

要说明的是,在运行 OSPF 协议的接口上才需要进行验证,并且运行 OSPF 协议双方的路由器都要有相同的配置,否则 OSPF 路由信息不能很好地交换。

(3) EIGRP 路由协议的验证

EIGRP 协议仅仅支持 MD5 认证。认证的配置有 3 个步骤:一是在端口配置模式使 MD5 认证模式生效;二是密钥链要一致;三是给密钥链配置密钥。

定义密钥链和密钥命令如下:

```
# key chain mykey
# key 1
# key-string xxx
# accept-lifetime 01: 00: 00 sep 9 199 infinite
# send-lifetime 01: 00: 00 sep 9 199 infinite
```

在端口配置模式使 MD5 认证模式生效命令如下:

```
# interface serial0.101 point-to-point
# ip address xxxx xxxx
# ip authentication mode eigrp 7 md5
# ip authentication key-chain eigrp 7 mykey
```

(4) 简单网管协议 SNMP 的安全

由于 SNMP 配置使用起来比较麻烦,一般使用较少。如果使用 SNMP 协议,对于其 public 和 private 的验证字一定要设置好。尤其是 private 的验证字,一定要是安全的、不易

猜测的，因为知道了它的验证字，就可以通过 SNMP 改变路由器的设置。

4. 路由器的网络安全配置

路由器除具有基本的路由功能以外，还有很多安全保护功能，用户要充分发挥路由器内在的安全性功能，更好地保护好网络安全。

(1) 物理结构的布局

如果路由器有一个以上的局域网端口，或几台路由器并行使用，可以根据访问性质进行分类。比如将供外部访问 WWW 服务器、FTP 服务器和 E-mail 服务器集中放在一个端口上，将企业内部的 WWW 服务器、FTP 服务器和数据库服务器放在路由器的其他端口上。这样便于对端口访问进行控制，对安全十分有利。即使黑客攻破了企业供外部访问的服务器，由于企业的其他机器和这些服务器不在同一个广播域，信息被窃听的可能性极低。

(2) 路由器的简单防火墙功能

目前，常用的路由器一般都有访问控制列表 ACL(access list)，即包过滤防火墙功能。访问列表可用于入口(inbound)，也可用于出口(outbound)。它可对源 IP 地址和目的 IP 地址以及协议端口号进行过滤，用它可以控制哪些网络可以访问什么服务器资源。使用 ACL 一般有创建一个路由表、指定接口和定义方向 3 个步骤。下面是一个配置实例。

```
# interface serial 0(指定串口 0)
# access - group 101 in(定义接口产生的过滤方向)
# access - list 101 deny ICMP any host 192.168.1.10 eq 8(阻止以 ICMP 回波请求的形式产生 Ping,
防止对主机 IP 地址的恶意窥视.ICMP 回波请求信息属于 ICMP 类型 8)
# access - list 101 permit ip any host 192.168.1.10(允许所有其他 IP 流向主机)
# access - list 101 deny ip any (拒绝所有不需要的访问)
```

5. 禁止路由器的部分网络服务的安全配置

(1) 禁止 Finger 服务

禁止 Finger 服务的命令如下：

```
Router(config)# no ip finger
Router(config)# no service finger
```

(2) 禁止 TCP、UDP Small 服务

禁止 TCP、UDP Small 服务的命令如下：

```
Router(config)# no service tcp - small - servers
Router(config)# no service udp - small - servers
```

(3) 建议禁止 HTTP 服务

禁止 HTTP 服务的命令为：

```
Router(config)# no ip http server
```

如果启用了 HTTP 服务则需要对其进行安全配置，比如设置用户名和密码和采用访问列表进行控制。

(4) 禁止 IP Source Routing

禁止 IP Source Routing 的命令为：

```
Router(config)# no ip source-route
```

(5) 禁止 ARP-Proxy 服务

如果不需要 ARP-Proxy 服务，则建议禁止它(路由器的默认状态是开启的)，其命令如下：

```
Router(config)# no ip proxy-arp
Router(config-if)# no ip proxy-arp
```

(6) 禁止 IP Directed Broadcast

禁止 IP Directed Broadcast 的命令为：

```
Router(config)# no ip directed-broadcast
```

(7) 禁止 IP Classless

禁止 IP Classless 的命令为：

```
Router(config)# no ip classless
```

(8) 禁止 ICMP 协议的 IP Unreachables、IP Redirects 和 IP Mask Replies

禁止 ICMP 协议的 IP Unreachables、IP Redirects 和 IP Mask Replies 的命令如下：

```
Router(config)# no ip unreachables
Router(config)# no ip Redirects
Router(config)# no ip Mask Replies
```

6. 路由器实现多设备控制端口访问的配置

如果有一台 Cisco 路由器加上异步模块或是一台具有内建异步串口的路由器，用户就可以在一个工作间或数据中心里全面实现对多个网络设备的控制连接。

对数据中心网络间的一台 Cisco 2511 路由器开始设置。当用户需要连接到网络设备的控制端口时，可以 Telnet 到控制台服务器，然后再 Telnet 到用户希望进行连接的设备，或者直接 Telnet 到设备控制端口。

用户可以采用更加先进的设备，如 Cisco 2610、3620、3640 或 3800 系列路由器来完成上述工作。

(1) 开始配置

先用 Cisco 2511 路由器的一个异步串行端口连接到用户的网络核心交换机、路由器和防火墙的每一个端口(这些设备各自同样需要具备串行控制口)；然后再按照以下 ip host 命令对新的 Cisco 终端服务器进行配置，以便使每个设备的连接变得简单：

```
ip host internet 2016 10.253.100.19
ip host gig_switch3 2015 10.253.100.19
ip host dmz_switch 2013 10.253.100.19
```

上述每一命令行的第三部分是设备端口号，其最后两个数字指定端口号。如第一台路由器(internet)后面的“2016”表示该路由器是在 16 号端口上。命令行的最后一部分是控制

台服务器的以太网端口 IP 地址。

用户还可以从 PC 直接连到这一设备。例如，可以从 PC 上 Telnet 到 10.253.100.19 2016。该命令指定 Telnet 客户端连接到 2016 端口而非默认的 Telnet 端口 23。

(2) 管理多个连接

在 Telnet 到控制台服务器并连接到这些设备后，用户需要知道如何才能在同一时间对多个连接进行管理。按照如下步骤进行操作：

① 在命令行中输入主机名称，即使用一个 IP 主机 Telnet 到用户配置过的设备上，这是 1 号连接。

② 在没有断开连接的情况下回到命令行，按下 Ctrl+Shift+6 键，然后按下 X 键，将显示控制台服务器提示符。

③ 在这里用户可以通过从 IP 主机列表中输入其主机名称 Telnet 到另一设备，这是 2 号连接。

④ 一旦连接到该路由器，再次按下 Ctrl+Shift+6 键，然后按下 X 键，将返回到控制台提示符。

⑤ 输入 show sessions 命令，可列出用户当前的会话。假设用户有两个会话：一个到第一台路由器，一个到第二台路由器。如果要取消其中某个会话，可输入 disconnect X，其中 X 为连接号码(“1”或“2”)。

⑥ 若要转到某个会话，输入 session number(“1”或“2”)即可。如果在空命令行中直接按回车键，可以回到上一个会话。

7. 实现精确控制访问的路由器配置

以 Cisco 2509 路由器(IOS 11.2)为例，介绍使用路由器实现精确控制访问的配置。

(1) 路由器设置

① 在路由器上指定可访问外界的 IP 地址

该步骤是通过设置路由器上的 IP 访问限制实现的，在 E0 端口(局域网端口)上添加一个访问列表(access-list)，只有指定了的 IP 地址允许进入：

```
Router#config terminal
Router(conf)#ip access-list 1 permit 192.168.1.11 0.0.0.0
Router(conf)#ip access-list 1 permit 192.168.1.12 0.0.0.0
Router(conf)#ip access-list 1 permit 192.168.1.19 0.0.0.0
Router(conf)#int e0
Router(conf-if)#ip access-group 1 in
Router(conf-if)#exit
Router(conf)#exit
Router#
```

然后，用 show access-list 命令查看：

```
Router#show ip access-list
Standard IP access list 1
Permit 192.168.1.11
Permit 192.168.1.12
Permit 192.168.1.19
```

可见，以上地址已写入访问列表，只有这些地址才能进入 E0 端口（局域网端口），从而进一步访问外界。

② 禁止外界访问内部的 Telnet 和 FTP 端口

在 E0 端口上添加一个访问列表，禁止进入 20、21 和 23 端口（20 和 21 为 FTP 端口，23 为 Telnet 端口）。

```
Router# config terminal
Router(conf)# ip access-list 101 deny tcp any any eq 23
Router(conf)# ip access-list 101 deny tcp any any eq 20
Router(conf)# ip access-list 101 deny tcp any any eq 21
Router(conf)# ip access-list 101 permit ip any any
Router(conf)# int e0
Router(conf-if)# ip access-group 101 out
Router(conf-if)# exit
Router(conf)# exit
Router#
```

用 show ip access-list 命令查看：

```
Router#  show ip access-list 101
Extended IP access list 101
Deny tcp any any eq 23
Deny tcp any any eq 20
Deny tcp any any eq 21
Permit ip any any
```

③ 防止授权 IP 地址的盗用

在路由器上建立一个静态 ARP 映射表：

```
Router# config terminal
Router(conf)# arp 192.168.1.11 0800.0900.0001 arpa
Router(conf)# arp 192.168.1.12 0800.0900.0002 arpa
Router(conf)# arp 192.168.1.19 0800.0900.0009 arpa
Router(conf)# exit
Router#
```

在 EXEC 态下用 show ip arp 命令查看：

```
Router#  show ip arp
Protocol Address Age(min)
Hardware Address Type Interface
Internet 192.168.1.11  -  0800.0900.0001 ARPA
Internet 192.168.1.1  -  0010.7b11.dd9f ARPA Ethernet0
Internet 192.168.1.12  -  0800.0900.0002 ARPA
Internet 192.168.1.19  -  0800.0900.0009 ARPA
Internet 192.168.1.22 9 0000.0c63.1300 ARPA
Internet 192.168.1.23 8 0000.0c36.6965 ARPA
```

其中，“-”标记已做了 ARP 静态映射的 IP 地址，192.168.1.1 是路由器 E0 口地址。

在做了 ARP 映射后，假设内部某一用户盗用了 192.168.0.11 IP 地址，但由于该用户机上网卡的硬件地址（MAC 地址）与 ARP 表中 192.168.9.11 所映射的 MAC 地址（0000.abcd.0009）不同，虽然该机器的 IP 地址允许进入路由器的 E0 端口，但所有返回的 TCP 包不能正确到达本机。因此，就达到了防止 IP 地址被盗用的目的。

④ 在 EXEC 命令态下用 copy run start 命令保存所做的修改

至此，Cisco 路由器设置完成。

（2）工作站配置

局域网中工作站的设置相对简单，步骤如下：

① 在菜单中选择“开始”→“设置”→“网络连接”→“本地连接”，单击“属性”命令后进入“本地连接 属性”对话框。

② 选定“TCP/IP 协议”选项（如图 2.3 所示）双击，或单击“属性”按钮，弹出“Internet 协议（TCP/IP）属性”对话框，如图 2.4 所示。



图 2.3　“本地连接 属性”对话框

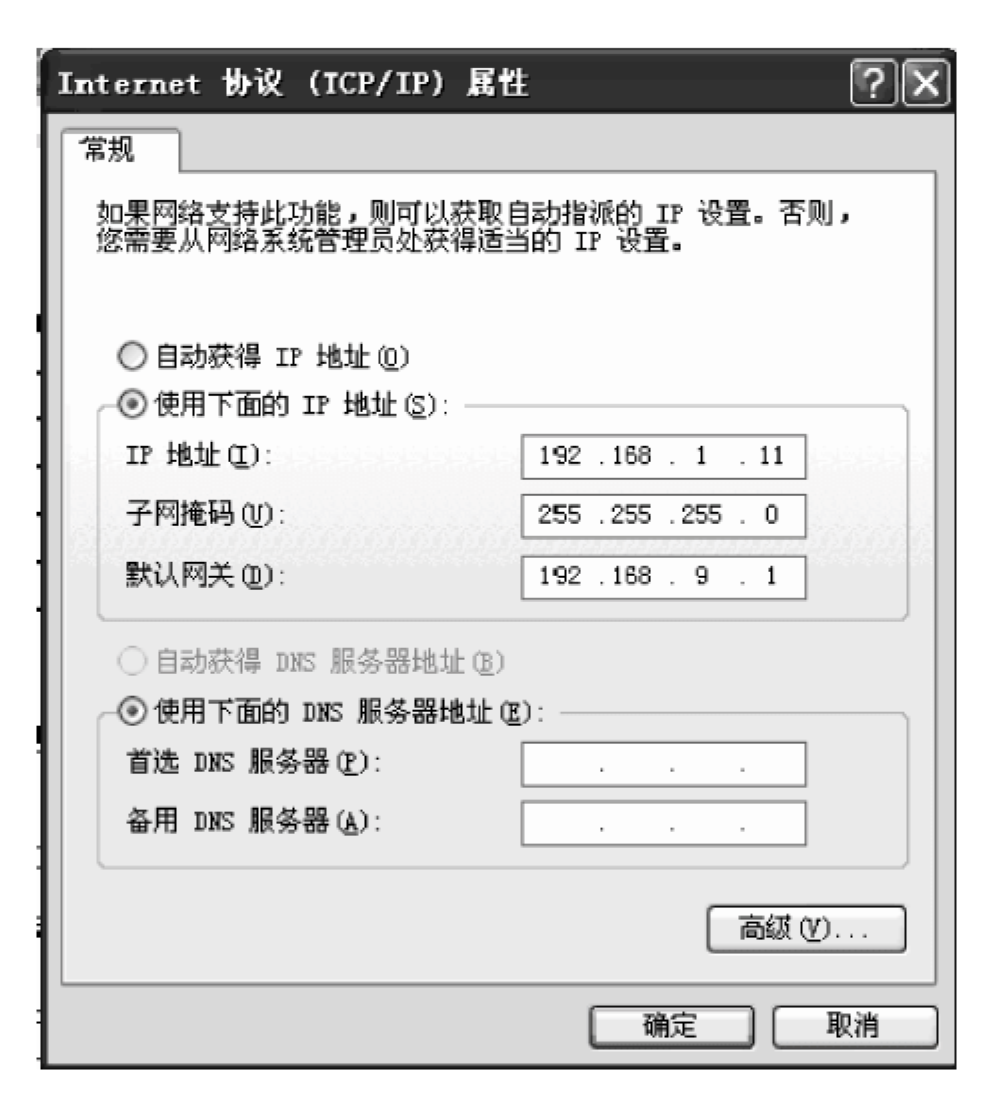


图 2.4　“Internet 协议（TCP/IP）属性”对话框

③ 选定“使用下面的 IP 地址”选项，在“IP 地址”和“子网掩码”文本框中填写 IP 地址（本例为 192.168.1.11）和子网掩码（255.255.255.0）。

④ 在默认“网关”项中，将路由器的 E0 地址（本例为 192.168.9.1）填入，作为默认网关。这一步对于能访问外界机器至关重要，因为在局域网中，路由器是与外界相连的唯一出口。

⑤ 选定“使用下面的 DNS 服务器地址”选项，填写“首选 DNS 服务器”和“备用 DNS 服务器”。

⑥ 单击“确定”按钮，重新启动计算机。

至此，完成了工作站的设置。

经过上述配置之后，局域网内的各个机器之间的访问是完全畅通的，只有部分授权的机器采用了指定 IP 地址之后才能够访问外界。路由器成为内部网络与外部 Internet 之间的唯一通道。

8. 路由器的其他安全配置

(1) IP 欺骗的简单防护

为防止对内部网络的 IP 欺骗,可过滤这样一些 IP 地址。比如过滤自己内部网络地址(201.120.30.0)、回环地址(127.0.0.0/8)、RFC1918 私有地址(172.16.0.0)、DHCP 自定义地址(169.254.0.0/16)、某文档作者测试用地址(192.0.2.0/24)、不用的组播地址(224.0.0.0/4)、SUN 公司的原测试地址(20.20.20.0/24;204.152.64.0/23)、全网络地址(0.0.0.0/8)的操作如下:

```
Router(config)# access-list 100 deny ip 201.120.30.0 0.0.0.255 any log
Router(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
Router(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
Router(config)# access-list 100 deny ip 169.254.0.0 0.0.255.255 any log
Router(config)# access-list 100 deny ip 192.0.2.0 0.0.0.255 any log
Router(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any log
Router(config)# access-list 100 deny ip 20.20.20.0 0.0.0.255 any log
Router(config)# access-list 100 deny ip 204.152.64.0 0.0.2.255 any log
Router(config)# access-list 100 deny ip 0.0.0.0 0.255.255.255 any log
```

(2) TCP SYN 的防范

通过访问列表防范 TCP SYN 的命令如下:

```
Router(config)# no access-list 106
Router(config)# access-list 106 permit tcp any 192.168.0.0 0.0.0.255 established
Router(config)# access-list 106 deny ip any any log
Router(config)# interface eth 0/2
Router(config-if)# description "external Ethernet"
Router(config-if)# ip address 192.168.1.254 255.255.255.0
Router(config-if)# ip access-group 106 in
```

通过 TCP 截获防范 TCP SYN 的命令如下:

```
Router(config)# ip tcp intercept list 107
Router(config)# access-list 107 permit tcp any 192.168.0.0 0.0.0.255
Router(config)# access-list 107 deny ip any any log
Router(config)# interface eth0
Router(config)# ip access-group 107 in
```

(3) Smurf 进攻的防范

防范 Smurf 进攻的命令如下:

```
Router(config)# access-list 108 deny ip any host 192.168.1.255 log
Router(config)# access-list 108 deny ip any host 192.168.1.0 log
```

(4) DDoS 攻击的防范

防范 DDoS 攻击的命令如下:

```
! The Trinoo DDos system
Router(config)# access-list 113 deny tcp any any eq 27665 log
Router(config)# access-list 113 deny udp any any eq 31335 log
```

```
Router(config)# access-list 113 deny udp any any eq 27444 log
!The Stacheldtraht DDos system
Router(config)# access-list 113 deny tcp any any eq 16660 log
Router(config)# access-list 113 deny tcp any any eq 65000 log
! The TrinityV3 system
Router(config)# access-list 113 deny tcp any any eq 33270 log
Router(config)# access-list 113 deny tcp any any eq 39168 log
! The Subseven DDos system and some Variants
Router(config)# access-list 113 deny tcp any any range 6711 6712 log
```

2.3　交换机安全与应用实践

2.3.1　交换机安全

交换机是一种基于MAC(网卡的硬件地址)识别,能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC地址,并把其存放在内部地址表中,通过在数据帧的源发送者和目标接收者之间建立临时的交换路径,使数据帧由源地址到达目的地址。

交换机在内部网中占有重要的地位,通常是整个网络的核心所在。在这个黑客入侵成风、病毒肆虐的网络时代,作为网络核心的交换机也理所当然要承担起网络安全的一部分责任。传统交换机主要用于数据包的快速转发,强调转发性能。交换机作为网络环境中重要的转发设备,其原来的安全特性已经无法满足现在的安全需求,因此,要求交换机应有专业安全产品的性能,安全交换机应运而生。在安全交换机中集成了安全认证、ACL、防火墙、入侵检测、防攻击、防病毒等功能。

1. 交换机基础

(1) 交换机功能

传统以太网交换机是第二层交换机,第二层交换机是一个可以将发送端地址与接收端地址连接起来的网络设备。该设备根据数据帧中的头信息,将来自一个或多个输入端口的帧送到一个或多个端口,完成数据交换。交换技术是作为对共享式局域网提供有效的网段划分解决方案而出现的,它可以使每个用户尽可能地分享到最大带宽。交换机工作在OSI模型中的数据链路层,因此交换机对数据包的转发是建立在MAC地址基础之上的,对于IP网络协议来说,它是透明的,即交换机在转发数据包时,不知道也无须知道信源机和信宿机的IP地址,只需知其物理地址(MAC地址)即可。显然,这种交换机的最大优点是数据交换快。因为它仅需要识别数据帧中的MAC地址,而直接根据MAC地址产生选择转发端口,算法又十分简单。但第二层交换机虽然也能支持子网的划分和广播限制等基本功能,但控制能力较小。

交换机在操作过程中会不断地收集信息去建立MAC地址表。MAC地址表说明了某个MAC地址是在哪个端口上被发现的,所以当交换机收到一个TCP/IP数据包时,会查看该数据包的目的MAC地址,然后核对自己的MAC地址表以确认应该从哪个端口把数据包发出去。此功能由按特定用户要求和特定电子系统的需要而设计、制造的专用集成电路

ASIC 完成,因此速度相当快,一般只需要几十微秒,交换机便可决定一个 IP 数据包该往哪里送。

当交换机收到一个目标地址未知的数据包(即 MAC 地址不能在其 MAC 地址表中找到)时,交换机会把 IP 数据包从它每一个端口中送出去。

交换机可看做是一个具有流量控制的网桥,它由背板、端口、缓冲区、逻辑控制单元和交叉矩阵等部件组成。

(2) 交换机的地址“学习”

交换机能够通过读取传送包的源 MAC 地址和记录帧进入交换机的端口来“学习”网络上每个设备的地址。然后,交换机把该信息加到它的转发数据库(MAC 地址表)中。地址“学习”是动态的,即当读取新 MAC 地址时它们被“学习”并存储在内容可寻址存储器(CAM)中。工作中如果读取到在 CAM 中没有登记“学习”的源地址,此 MAC 地址被“学习”并存储到 CAM 中,以备将来使用。

每次存储地址时,地址被打上一个时间标记。如果在一段时间内都没有被使用过的 MAC 地址将从 MAC 列表中删除。通过这个时间标记来保证删除过时的地址和保持最新的地址。CAM 维护了一个精确和有用的转发数据库,即 MAC 地址表。

(3) 交换机的转发与过滤

当主机 A 发一个帧给主机 B 时,由于目的 MAC 地址(主机 B 的 MAC 地址)已在 MAC 地址表中存在对应项,故交换机会将此帧直接发到 B 所在交换机的端口,而不会再将帧发往其他端口,这样就节省了其他端口上的带宽,这就是所谓的转发与过滤。

但是对于广播和组播,交换机通常是把广播帧或组播帧向所有端口转发,不管 MAC 地址表是否完整。而一个交换机永远“学习”不到广播或组播地址,因为它们永远不会出现在一个帧的源地址中。所以第二层的交换机无法控制广播域,用交换机分割的网段虽然处于不同的冲突域,但仍然处于同一个广播域中。因此,需要第三层设备(如第三层交换机、路由器)来分割广播域。

2. 交换机安全

(1) 安全交换机三层含义

交换机最重要的作用就是转发数据。在黑客攻击和病毒侵扰下,交换机要能够继续保持其高效的数据转发速率不受到攻击的干扰,这就是交换机所需的最基本的安全功能。同时,交换机作为整个网络的核心,应该能对访问和存取网络信息的用户进行区分和权限控制。更重要的是,交换机还应该配合其他网络安全设备,对非授权访问和网络攻击进行监控和阻止。

(2) 安全交换机的新功能

① 802.1x 安全认证

在传统的局域网环境中,只要有物理的连接端口,未经授权的网络设备就可以接入局域网,或者未经授权的用户就可以通过连接到局域网的设备进入网络。这样就造成了潜在的安全威胁。另外,在学校和智能小区的网络中,由于涉及网络的计费,所以验证用户接入的合法性也显得非常重要。IEEE 802.1x 正是解决这个问题的良方,目前已经被集成到二层智能交换机中,完成对用户的接入安全审核。

802.1x 协议是基于端口的访问控制协议。它能够在利用 IEEE 802 局域网优势的基础上提供一种对连接到局域网的用户进行认证和授权的手段，达到接受合法用户接入，保护网络安全的目的。802.1x 协议与 LAN 是无缝融合的。802.1x 利用了交换式 LAN 架构的物理特性，实现了 LAN 端口上的设备认证。在认证过程中，LAN 端口要么充当认证者，要么扮演请求者。在作为认证者时，LAN 端口在需要用户通过该端口接入相应的服务之前，首先进行认证，如若认证失败则不允许接入；在作为请求者时，LAN 端口则负责向认证服务器提交接入服务申请。基于端口的 MAC 锁定只允许信任的 MAC 地址向网络中发送数据。来自任何“不信任”的设备的数据流会被自动丢弃，从而确保最大限度的安全性。

在 802.1x 协议中，只有具备了以下三个元素才能够完成基于端口的访问控制的用户认证和授权。

- 客户端。客户端一般安装在用户的工作站上，当用户有上网需求时，激活客户端程序，输入必要的用户名和口令，客户端程序将会送出连接请求。
- 认证系统。在以太网系统中认证系统就是指认证交换机，其主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口。
- 认证服务器。认证服务器通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的网络服务，并根据认证结果向交换机发出打开或保持端口关闭的命令。

② 流量控制

安全交换机的流量控制技术把流经端口的异常流量限制在一定的范围内，避免交换机的带宽被无限制滥用。安全交换机的流量控制功能能够实现对异常流量的控制，避免网络堵塞。

③ 防范 DDoS 攻击

企业网一旦遭到分布式拒绝服务（DDoS）攻击，会影响大量用户的正常使用，严重时甚至造成网络瘫痪。安全交换机采用专门技术来防范 DDoS 攻击，它可以在不影响正常业务的情况下，智能地检测和阻止恶意流量，从而防止网络受到 DDoS 攻击的威胁。

④ 虚拟局域网 VLAN

虚拟局域网是安全交换机必不可少的功能。VLAN 可以在二层或三层交换机上实现有限的广播域。它可把网络分成一个个独立的区域，控制这些区域是否可以通信。VLAN 可能跨越一个或多个交换机，设备之间好像在同一个网络间通信一样，与它们的物理位置无关。VLAN 可在各种形式上形成，如端口、MAC 地址、IP 地址等。VLAN 限制了各个不同 VLAN 之间的非授权访问，而且可以设置 IP 地址与 MAC 地址绑定功能限制用户非授权访问网络。

⑤ 基于 ACL 的防火墙功能

安全交换机采用了访问控制列表（ACL）来实现包过滤防火墙的安全功能，增强安全防范能力。ACL 通过对网络资源的访问控制，确保网络设备不被非法访问或被作为攻击跳板。ACL 是一张规则表，交换机按照顺序执行这些规则，并且处理每一个进入端口的数据包。每条规则根据数据包的属性（如源地址、目的地址和协议）允许或拒绝数据包通过。由于规则是按照一定顺序处理的，因此每条规则的相对位置对于确定允许和不允许什么样的数据包通过网络至关重要。ACL 以前只在核心路由器才有使用。在安全交换机中，访问控

制过滤措施可以基于源/目标交换槽、端口、源/目标 VLAN、源/目标 IP、TCP/UDP 端口、ICMP 类型或 MAC 地址来实现。

⑥ IDS 功能

安全交换机的入侵检测系统(IDS)功能可以根据上报信息和数据流内容进行检测,在发现网络安全事件时,进行有针对性的操作,并将这些对安全事件反应的动作发送到交换机上,由交换机来实现精确的端口断开操作。实现这种联动,需要交换机支持认证、端口镜像、强制流分类、进程数控制、端口反向查询等功能。

(3) 安全交换机的配置

安全交换机的出现,使得网络在交换机层次上的安全能力大大增强。安全交换机可以配备在网络的核心位置上,如 Cisco 的 Catalyst 6500 模块化的核心交换机。这样就可以在核心交换机上统一配置安全策略,做到集中控制,方便网络管理人员的监控和调整。

把安全交换机放在网络的接入层或汇聚层是另外一个选择。这样配备安全交换机的方式的核心就是把权力下放到边缘,在各个边缘就开始实施安全交换机的性能,把入侵和攻击以及可疑流量阻挡在边缘之外,确保全网的安全。这样就需要在边缘配备安全交换机,很多厂家已经推出了各种边缘或汇聚层使用的安全交换机。它们就像一个个堡垒一样,在核心周围建立起一道坚固的安全防线。

2.3.2 交换机的安全配置实践

配置交换机使网络对可访问站点进行控制,从而实现对自身的保护。如果用户的工作站是固定的,那么往往可以通过 MAC 地址与相同接入层的交换机端口连接。如果工作站是移动的站点,也可以动态地获得其 MAC 地址并将该地址加入到一个地址列表中,以实现与交换机端口的连接。

端口安全(port-secure)命令定义了一个最大值,即在 MAC 地址表中与交换机端口相联系的所允许的最多目的 MAC 地址。最大计数值范围从 1~132,默认值为 132,即最多可有 132 个目的 MAC 地址。

用 port-secure 命令设置端口安全性后,该端口所对应的地址出现在 MAC 地址表中,不会以动态类型出现。因为若该端口对应的静态 MAC 地址数未达到最大计数值,且交换机又从端口的帧流量源地址中学到了新的地址,则将该地址自动转变成永久 MAC 地址存入 MAC 地址表中。一旦永久或静态 MAC 地址数达到 count 值,则不再接受新的地址,这种方式称为 Sticky-Learns(记忆性学习)。该方式解决了未经允许而多人共用一台集线器接入交换机的一个端口所造成的不安全因素。

1. MAC 地址表及相关信息的设置

MAC 地址表对于交换机而言如同路由表对于路由器一样。因此,对 MAC 地址表的配置也尤为重要。

(1) 显示 MAC 地址表

MAC 地址表中的地址由永久地址、限制性静态地址和动态地址三种地址组成。

在 Switch# show MAC-address-table 命令中即可看到 MAC 地址表。

MAC 地址表由地址、源端口表、目的端口和类型组成。

① 地址。目的 MAC 地址。

② 源端口表。可以向目的端口转发帧的源端口集合。

③ 目的端口。从目的端口转发数据帧,即可到达符合目的 MAC 地址的主机。

④ 类型。动态地址意味着 MAC 地址表中的地址是通过学习流入该端口的数据帧的帧头中的源端 MAC 地址得来的(即交换机的学习功能)。该表项必须被不断更新(即有流量通过),否则一段时间后该表项被自动删除。

如 Cisco 1900 交换机最多可在表中容纳 1024 个 MAC 地址,一旦 MAC 地址表被填满,除非有表项超时被自动删除,否则新地址不能加入。

(2) 设置永久地址

若设置了永久地址的目的 MAC 地址及其转发端口,则该地址永久不会超时,所有的端口均可以转发帧给它。设置命令如下:

```
Switch(config)#MAC-address-table permanent[MAC Address][type slot/port]
```

(3) 设置限制性静态地址

限制性静态地址不但继承了永久地址的所有特性,更进一步严格限制了源端口,安全性得到进一步增强。设置限制性静态地址的命令如下:

```
Switch(config)#MAC-address-table restricted static[MAC address][type slot/port][source interface list]
```

(4) 删除表项

如果不需要某条 MAC 地址表项,则可将其删除,命令如下:

```
Switch#clear MAC-address-table[dynamic|permanent|restricted]
```

2. 配置交换机端口

(1) 认证端口

可以给交换机端口配置增加一个文本描述来帮助认证配置,这个描述仅仅意味着一个注释域,作为端口使用的一条记录或者其他唯一的信息。为了给端口分配一个注释或描述,在接口配置模式下输入如下命令:

```
Switch(config-if)#description description-string
```

执行接口配置命令 no description 时删除一个注释或描述。

(2) 端口速度

可以通过交换机配置命令给交换机端口指定一个特殊的速度,快速以太网 10/100 端口可以为自协商模式,设置速度为 10、100 或 Auto(默认)。使用如下命令可在一个特殊的以太网端口上指定端口速度:

```
Switch(config-if)#speed{10 | 100 | auto}
```

(3) 端口模式

可以为一个以太网交换机端口指定一个特殊的连接模式,使端口在半双工、全双工或自协商模式下操作。在接口配置模式下输入如下命令可在交换机端口上设置连接模式:

```
Switch(config-if)#duplex{auto | full | half}
```

在接口配置模式下执行 description 命令，可配置描述信息。

在 Cisco 1900 下的描述信息不能使用空格键，如：

```
1900(config)#int e0/1
1900(config-if)#description Cisco_VLAN
1900(config-if)#int f0/26
1900(config-if)#description trunk-to-building_4
1900(config-if)#
```

在 Cisco 2950 下的描述可以使用空格键，如：

```
2950(config)#int fa 0/1
2950(config-if)#description Sales Printer
2950(config-if)#^Z
```

可以执行 show interface 和 show running-config 命令来查看这些描述信息。

3. 交换机口令的安全配置

通常，网络设备应该配置为对于未被授权的访问是安全的。Cisco 交换机通常提供一个简单安全的形式，通过设置密码来限制注册到用户接口的人。交换机有用户模式和特权模式两种可用的用户访问级别。用户模式是访问的第一级密码，它允许访问基本的端口。特权模式是第二级密码，它允许设置或改变交换机操作参数和配置。

(1) 密码设置

为用户模式设置注册密码，需要在全局配置模式下输入下列命令：

```
Switch(config)#line con 0
Switch(config-line)#password password
Switch(config-line)#login
Switch(config-1)#line vty 0 15
Switch(config-line)#password password
Switch(config-line)#login
```

登录密码(用户模式)可防止未授权用户登录。启用密码(特权模式)可防止未授权用户修改配置。

对于 Catalyst 1900 交换机，在 Cisco 1900 下输入 enable 进入特权模式，再输入 configt 进入全局配置模式：

```
>en
#configt
(config)#
```

当进入全局配置模式后，可使用 enable password 命令配置登录密码和启用密码：

```
(config)#enable password?
level Set exec level password
(config)#enable password level
<1-15>Level Number
```

level 1 为登录密码，level 15 为启用密码，密码长度范围是 4～8 个字符，如果超过此范围，系统则提示密码长度无效，如：

```
(config) # enable password level 1 nocoluvsnoko
Error: Invalid password length.
Password must be between 4 and 8 characters
```

(2) 重配置并验证

```
(config) # enable password level 1 noco
(config) # enable password level 15 noko
(config) # exit
#exit
```

对 Catalyst 2950 交换机的配置与路由器的配置有点类似，如：

```
Switch> en
Switch# conft
Switch(config) # line?
<0-16> First Line number
console Primary terminal line
vty Virtual terminal
Switch(config) # line vty?
<0-15> First Line number
Switch(config) # line vty 0 15
Switch(config-line) # login
Switch(config-line) # password noko
Switch(config-line) # line con 0
Switch(config-line) # login
Switch(config-line) # password noco
Switch(config-line) # exit
Switch(config) # exit
Switch#
```

enable secret 比 enable password 更安全，如果同时设置了两者，则只有前者起作用。注意，在 Catalyst 1900 交换机中，enable secret 和 enable password 可以设置成一样的，如：

```
(config) # enable secret noko
```

Catalyst 2950 交换机的配置和路由器类似，但是 enable secret 和 enable password 不可以设置成一样的，如：

```
Switch(config) # enable password noko
Switch(config) # enable secret noko
The enable secret you have chosen is the same as your enable password.
This is not recommended. Reenter the enable secret.
Switch(config) # enable secret noco
Switch(config) #
```

4. 交换机端口安全配置方案与操作

Cisco 交换机提供了对端口进行保护的功能，该功能基于 MAC 地址控制对端口的访

问。要在一个接入层的交换机(用户接入的交换机)端口配置端口保护,首先用下面的接口配置命令在端口上激活保护功能:

```
Switch(config-if)#switchport port-security
```

在各个应用端口被保护的接口,可以用如下接口配置命令规定被允许访问的 MAC 地址的最大数目:

```
Switch(config-if)#switchport port-security maximum max-address
```

默认情况下,各个交换机端口仅允许一个 MAC 地址对其进行访问。可以设定的地址数目范围是 1~1024。默认设置时,使用端口保护的接口是动态获得 MAC 地址的。还可以在接口上静态定义一个或多个 MAC 地址,这些地址都可以通过端口进行网络的访问。静态地址可以用下面的接口配置命令定义:

```
Switch(config-if)#switchport port-security MAC-address MAC-address
```

最后,必须确定使用端口保护的接口,在遇到违法的 MAC 地址时可以用如下接口配置命令进行这项设置:

```
Switch(config-if)#switchport port-security violation{shutdown | restrict | protect}
```

违法是指获得超过最大数目的 MAC 地址,或者一个未知的(非静态定义的)MAC 地址试图访问端口。

配置 Cisco 交换机端口安全具体可有 3 种方案供选择。方案 1 和方案 2 实现的功能类似,可在具体的交换机端口上绑定特定的主机的 MAC 地址(网卡硬件地址),方案 3 是在具体的交换机端口上同时绑定特定的主机的 MAC 地址(网卡硬件地址)和 IP 地址。

(1) 配置方案 1——基于端口的 MAC 地址绑定

现以 Cisco 2950 交换机为例进行配置。登录进入 Cisco 交换机,输入管理口令进入配置模式,输入如下命令:

```
Switch#config terminal                          #进入配置模式
Switch(config)Interface fastethernet 0/1        #进入具体端口配置模式
Switch(config-if)Switchport port-security       #配置端口安全模式
Switch(config-if )switchport port-security MAC-address MAC-address
                                                #配置该端口要绑定的主机的 MAC 地址
Switch(config-if )no switchport port-security MAC-address MAC-address
                                                #删除绑定主机的 MAC 地址
```

注意:以上命令可使交换机上某个端口绑定一个具体主机的 MAC 地址,这样只有该主机可以使用网络,如果对该主机的网卡进行了更换或其他 PC 想通过该端口使用网络都是不可行的,除非删除或修改该端口上绑定的 MAC 地址。

以上设置适用于 Cisco 2950、3550、4500、6500 系列交换机。

(2) 配置方案 2——基于 MAC 地址的扩展访问列表

登录进入 Cisco 交换机,输入如下命令:

```
Switch(config)Mac access-list extended MAC10
  #定义一个 MAC 地址访问控制列表并且命名该列表为 MAC10
```

```
Switch(config)permit host 0009.6bc4.d4bf any
  #定义 MAC 地址为 0009.6bc4.d4bf 的主机可以访问任意主机
Switch(config)permit any host 0009.6bc4.d4bf
  #定义所有主机可以访问 MAC 地址为 0009.6bc4.d4bf 的主机
Switch(config-if)interface Fa0/20 #进入配置具体端口的模式
Switch(config-if)mac access-group MAC10 in
  #在该端口上应用名为 MAC10 的访问列表
Switch(config)no mac access-list extended MAC10
  #清除名为 MAC10 的访问列表
```

此配置功能与方案 1 大体相同，但它是基于端口的 MAC 地址访问控制列表限制，可以限定特定源 MAC 地址与目的地址范围。

以上配置功能在 Cisco 2950、3550、4500、6500 系列交换机上均可实现，但需注意的是 Cisco 2950、3550 需要交换机运行增强的软件镜像(enhanced image)。

(3) 配置方案 3——IP 地址与 MAC 地址绑定

将方案 1 或方案 2 与基于 IP 的访问控制列表组合可实现 IP 地址与 MAC 地址绑定。

```
Switch(config)mac access-list extended MAC10
  #定义一个 MAC 地址访问控制列表并且命名该列表为 MAC10
Switch(config)permit host 0009.6bc4.d4bf any
  #定义 MAC 地址为 0009.6bc4.d4bf 的主机可以访问任意主机
Switch(config)permit any host 0009.6bc4.d4bf
  #定义所有主机可以访问 MAC 地址为 0009.6bc4.d4bf 的主机
Switch(config)ip access-list extended IP10
  #定义一个 IP 地址访问控制列表并且命名该列表为 IP10
Switch(config)permit 192.168.0.1 0.0.0.0 any
  #定义 IP 地址为 192.168.0.1 的主机可以访问任意主机
Switch(config)permit any 192.168.0.1 0.0.0.0
  #定义所有主机可以访问 IP 地址为 192.168.0.1 的主机
Switch(config-if)interface Fa0/20
  #进入配置具体端口的模式
Switch(config-if)mac access-group MAC10 in
  #在该端口上应用名为 MAC10 的访问列表(即前面定义的访问策略)
Switch(config-if)ip access-group IP10 in
  #在该端口上应用名为 IP10 的访问列表(即前面定义的访问策略)
Switch(config)no mac access-list extended MAC10 in
  #清除名为 MAC10 的访问列表
Switch(config)no ip access-group IP10 in
  #清除名为 IP10 的访问列表
```

方案 1 是基于主机 MAC 地址与交换机端口的绑定，方案 2 是基于 MAC 地址的访问控制列表。将方案 1 或方案 2 与 IP 访问控制列表结合起来使用以达到绑定 IP 与 MAC 地址的目的。

5. 交换机端口与主机地址的安全配置

最常用的对端口安全的理解就是可根据 MAC 地址进行对网络流量的控制和管理，比如 MAC 地址与具体的端口绑定，限制具体端口通过的 MAC 地址的数量，或者在具体的端口不允许某些 MAC 地址的帧流量通过。

(1) MAC 地址与端口绑定

当发现主机的 MAC 地址与交换机上指定的 MAC 地址不同时，交换机相应的端口将关闭。当给端口指定 MAC 地址时，端口模式必须为 access 或者 trunk 状态。MAC 地址与端口绑定的操作如下：

```
3550 - 1＃conf t
3550 - 1(config)＃int f0/1
3550 - 1(config - if)＃switchport mode access
  ＃指定端口模式
3550 - 1(config - if)＃switchport port - security mac - address 00 - 90 - F5 - 10 - 79 - C1
  ＃配置 MAC 地址
3550 - 1(config - if)＃switchport port - security maximum 1
  ＃限制此端口允许通过的 MAC 地址数为 1
3550 - 1(config - if)＃switchport port - security violation shutdown
  ＃当发现与上述配置不符时，将端口关闭
```

(2) 通过 MAC 地址来限制端口流量

此配置允许一个 trunk 端口最多通过 100 个 MAC 地址，超过 100 时，来自新主机的数据帧将丢失。限制端口流量的 MAC 地址配置操作如下：

```
3550 - 1＃conf t
3550 - 1(config)＃int f0/1
3550 - 1(config - if)＃switchport trunk encapsulation dot1q
3550 - 1(config - if)＃switchport mode trunk
  ＃配置端口模式为 trunk
3550 - 1(config - if)＃switchport port - security maximum 100
  ＃允许此端口通过的最大 MAC 地址数目为 100
3550 - 1(config - if)＃switchport port - security violation protect
  ＃当主机 MAC 地址数目超过 100 时，交换机继续工作，但来自新的主机的数据帧将丢失
```

上述配置可根据 MAC 地址来允许流量，如下的配置则是根据 MAC 地址来拒绝流量。

```
3550 - 1＃conf t
3550 - 1(config)＃mac - address - table static 00 - 90 - F5 - 10 - 79 - C1 vlan 2 drop
  ＃在相应的 VLAN 丢弃流量
3550 - 1＃conf t
3550 - 1(config)＃mac - address - table static 00 - 90 - F5 - 10 - 79 - C1 vlan 2 int f0/1
  ＃在相应的接口丢弃流量
```

(3) 可靠的 MAC 地址配置类型

可靠的 MAC 地址配置有如下 3 种类型。

① 静态可靠的 MAC 地址

在交换机接口模式下手动配置，该配置会被保存在交换机 MAC 地址表和运行配置文件中，交换机重新启动后不丢失（当然是在保存配置完成后）。静态可靠的 MAC 地址的命令步骤如下：

```
Switch＃config terminal
Switch(config)＃interface interface - id          ＃进入需要配置的端口
Switch(config - if)＃switchport mode Access       ＃设置为交换模式
```

```
Switch(config-if)#switchport port-security   #打开端口安全模式
Switch(config-if)#switchport port-security violation {protect | restrict | shutdown }
```

上一条命令是可选的，可以不用配置，默认的是 shutdown 模式，但是在实际配置中推荐使用 restrict。

```
Switch(config-if)#switchport port-security maximum value
```

上一条命令也是可选的，可以不用配置，默认的 maximum 是一个 MAC 地址，Cisco 2950 和 3550 交换机的这个最大值是 132。

② 动态可靠的 MAC 地址

这是交换机默认的类型。在这种类型下，交换机会动态学习 MAC 地址，但是该配置只会保存在 MAC 地址表中，不会保存在运行配置文件中，并且交换机重新启动后，这些 MAC 地址表中的 MAC 地址会被自动清除。动态可靠的 MAC 地址配置是交换机默认的设置，这里不再介绍其步骤。

③ 黏性可靠的 MAC 地址

这种情况下可以手动配置 MAC 地址和端口的绑定，也可以让交换机自动学习来绑定。该配置会被保存在 MAC 地址中和运行配置文件中。如果保存配置，交换机重启动后不用再自动重新学习 MAC 地址。黏性可靠的 MAC 地址配置的命令步骤如下：

```
Switch#config terminal
Switch(config)#interface interface-id
Switch(config-if)#switchport mode Access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security violation {protect | restrict | shutdown }
Switch(config-if)#switchport port-security maximum value
```

上面几条命令的解释与静态的原因相同，不再说明。

```
Switch(config-if)#switchport port-security mac-address sticky
```

上一条命令就说明是配置为黏性可靠的 MAC 地址。

6. 交换机访问控制的安全配置

作为网络中应用最为广泛的交换机，要能开发其安全特性，以有效地保护对网络的访问，一些组织和厂商也纷纷提出自己的安全策略。现在通过多层交换机特性来提高网络的安全性和对带宽的控制已经相当地普遍。随着一些安全特性如访问控制列表(ACL)和 IEEE 802.1x 标准已经成为许多厂商产品的标准，一些使用者开始把它们作为网络设施安全的一个单独增加的层次。

ACL 通过对网络资源进行访问输入和输出控制，确保网络设备不被非法访问或被作为攻击跳板。ACL 是一张规则表，交换机按照顺序执行这些规则，并且处理每一个进入端口的数据包。每条规则根据数据包的属性(如源地址、目的地址和协议)要么允许、要么拒绝数据包通过。由于规则是按照一定顺序处理的，因此每条规则的相对位置对于确定允许和不允许什么样的数据包通过网络至关重要。如下操作（192.168.1.2 和 192.168.1.1 分别为两个主机的 IP 地址）：

```
Switch(config)#access-list 1 permit host 192.168.1.2
Switch(config)#access-list 1 deny any
Switch(config)#int vlan 1
Switch(config-vlan)ip access-group 1 out
Switch(config-vlan)ip access-group 1 in
Switch(config)#access-list 2 permit host 192.168.1.1
Switch(config)#access-list 2 deny any
Switch(config)#int vlan 2
Switch(config-vlan)ip access-group 2 out
Switch(config-vlan)ip access-group 2 in
```

2.4 服务器安全

在基于服务器的网络中，网络服务器担负着向客户机提供信息数据、网络存储、科学计算和打印等共享资源和服务，并负责协调管理这些资源。由于网络服务器要同时为网络上所有的用户服务，因此，要求网络服务器具有高可靠性、高吞吐能力、大内存容量和较快的处理速度等性能。

一般选用高性能计算机作为服务器。从保证网络稳定、可靠、安全运行方面看，服务器涉及的技术较多，常见的服务器技术有多处理器技术、热插拔技术、集群技术、ISC 技术和 EMP 技术等。

2.4.1 网络服务器

根据网络的应用和规模，网络服务器可选用高档微机、工作站、PC 服务器、小型机、中型机和大型机等。根据网络服务器的不同功能和不同应用，可将服务器分成不同类型。

按照服务器用途，服务器可分为文件服务器、数据库服务器、Internet/Intranet 通用服务器、应用服务器等，主要用于完成网络不同的功能。

1. 文件服务器

计算机网络诞生初期，最原始的一种基本应用模式是资源共享，其功能体现在利用服务器的海量存储和优秀的吞吐能力，为网络中连接的工作站提供共享服务，包括建立共享文档库、共享程序库，以及建立在并发控制和冲突控制基础上的文件型数据服务等。文件服务器已经拥有比较完备的磁盘设备管理和用户安全管理体系。

2. 数据库服务器

分布式协同信息处理是目前计算机网络应用的核心之一，也是资源共享的延伸。数据库服务器用于安装大型数据库系统的服务程序，如 Oracle、SQL Server 和 Informix 等，以便为各客户应用提供所需的数据。

3. Internet/Intranet 通用服务器

Internet/Intranet 通用服务器用于在异构网络环境下统一简化的客户端平台和广域网

互通互连基础上的信息发布、采集、利用和高度资源共享，是现阶段用户使用最多的网络服务应用类型。这类服务器主要有 Web 服务器、电子邮件服务器、DNS 服务器和目录服务器等。

4. 应用服务器

应用服务器用于在通用服务器硬件平台上安装相应的应用服务软件并实现特定的功能，如数据中间件服务器、流式媒体点播服务器、电视会议服务器和打印服务器等。

2.4.2　服务器的安全设置

1. 服务器的安全策略

(1) 对服务器进行安全设置(包括 IIS 的相关设置、Internet 各服务器的安全设置、MySQL 安全设置等)，提高服务器应用的安全性。

(2) 进行日常的安全检测(包括查看服务器状态、检查当前进程情况、检查系统账号、查看当前端口开放情况、检查系统服务、查看相关日志、检查系统文件、检查安全策略是否更改、检查目录权限、检查启动项等)，以保证服务器正常、可靠地工作。

(3) 加强服务器的日常管理(包括服务器的定时重启、安全和性能检查、数据备份、监控、相关日志操作、补丁修补和应用程序更新、隐患检查和定期的管理密码更改等)。

(4) 采取安全的访问控制措施，保证服务器访问的安全性。

(5) 禁用不必要的服务，提高安全性和系统效率。

(6) 修改注册表，使系统更强壮(包括隐藏重要文件/目录、修改注册表实现完全隐藏、启动系统自带的 Internet 连接防火墙、防止 SYN 洪水攻击、禁止响应 ICMP 路由通告报文、防止 ICMP 重定向报文攻击、修改终端服务端口、禁止 IPC 和建立空链接、更改 TTL 值、删除默认共享等)。

(7) 正确划分文件系统格式，选择稳定的操作系统安装盘。

(8) 正确设置磁盘的安全性(包括系统盘权限设置、网站及虚拟机权限设置、数据备份盘和其他方面的权限设置)。

2. 服务器的安全设置实践

(1) 安装补丁

经常访问 Microsoft 和一些安全站点，下载最新的 Service Pack 和漏洞补丁，是保障服务器安全的有效方法。

安装好操作系统之后，最好能在托管之前就完成补丁的安装。配置好网络后，如果是 Windows 2000 系统，则确定安装上 SP4；如果是 Windows 2003 系统，则要装上 SP1 或 SP2，然后启动 WindowsUpdate，安装所有的关键更新。

(2) 安装防病毒软件

在系统使用前最好安装上一款防病毒软件。不论是选择诺顿、瑞星金山、卡巴斯基，还是别的防病毒软件，随用户的意愿。当然，任何防病毒软件都不能查杀所有的病毒(木马)，如 ASP 木马的特征可以通过一定手段来避开防病毒软件的查杀，因此，实际使用中还应配

以其他的安全手段。

(3) 禁止建立空链接

默认情况下,任何用户都可通过空链接连上服务器,进而猜测账号,枚举出密码。可通过修改注册表来禁止建立空链接。其操作很简单,单击“开始”→“运行”命令,输入 regedit,确认后进入注册表后,把“HKEY_Local_Machine\System\CurrentControlSet\Control\LSA-RestrictAnonymous”的键值改成“1”即可。

(4) 关闭不必要的端口

关闭端口意味着减少功能,用户应根据自己的实际应用在安全和功能两方面要求上权衡利弊,进行取舍。如果服务器安装在防火墙的后面,风险就会少些。但无论如何开放的端口安全风险总是存在的。用户可用端口扫描器扫描系统已开放的端口,确定系统开放的哪些服务可能引起黑客入侵。在系统目录中的\system32\drivers\etc\services 文件中有知名端口和服务的对照表可供参考。为了网络服务器的安全,可考虑关闭自己端的 139 端口、445 端口、3389 端口、4899 端口等。

① 关闭 139 端口

139 端口是 NetBIOS 协议所使用的会话服务端口,在安装了 TCP/IP 协议的同时,NetBIOS 也会被作为默认设置安装到系统中。该端口的开放意味着硬盘可能会在网络中共享,网上黑客可通过 NetBIOS 了解用户计算机中的一切。在以前的 Windows 版本中,只要不安装 Microsoft 网络的文件和打印共享协议,就可关闭 139 端口。但在 Windows Server 2003 系统中,要单独进行关闭 139 端口的操作才行。关闭 139 端口的具体步骤如下:

- 单击“开始”→“设置”→“网络连接”→“本地连接”→“属性”→“Internet 协议(TCP/IP)”命令,打开“本地连接属性”窗口。
- 去掉“Microsoft 网络的文件和打印机共享”前面的“√”,如图 2.5 所示。

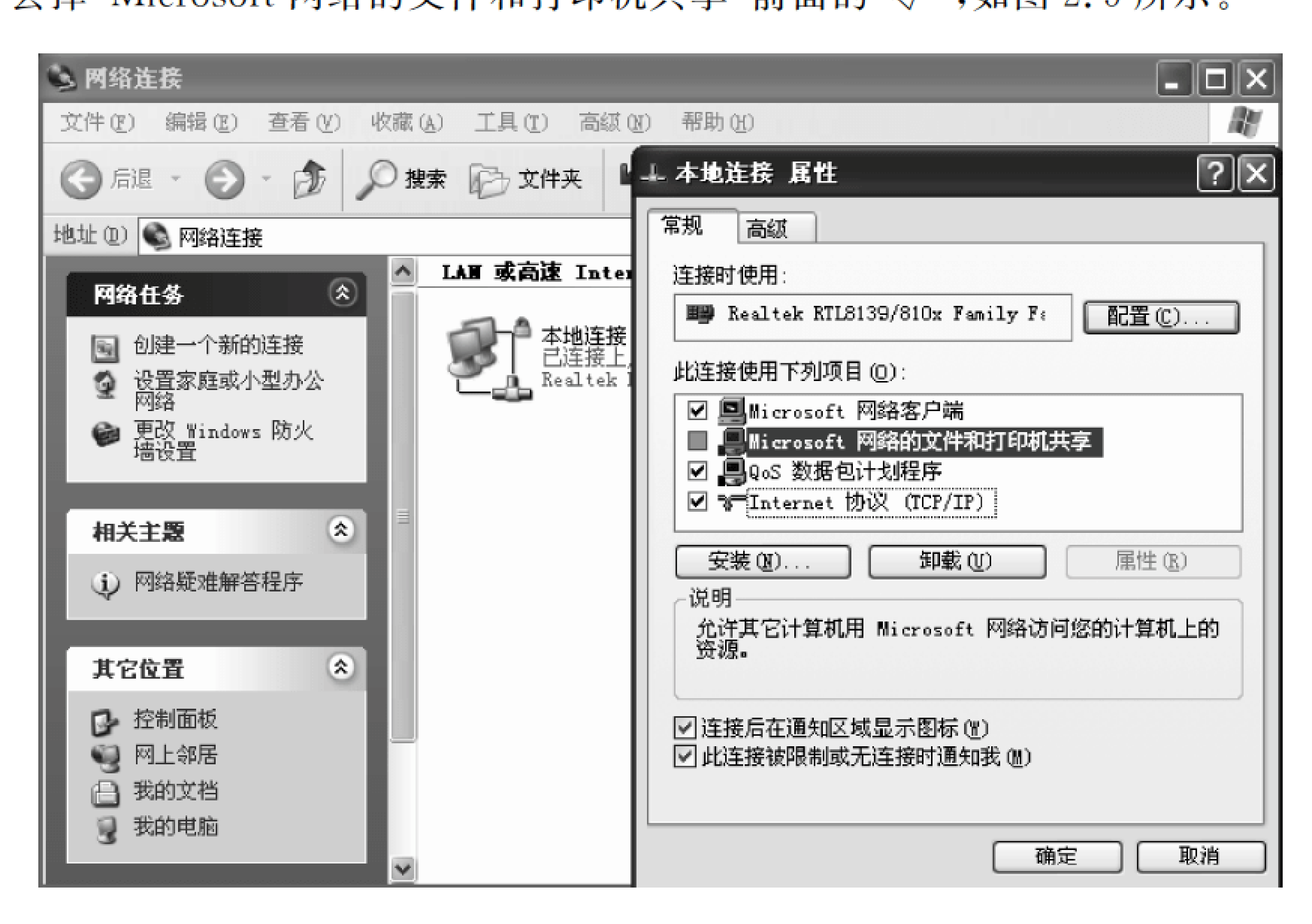


图 2.5 取消选中“Microsoft 网络的文件和打印机共享”

• 选中“Internet 协议(TCP/IP)”选项，依次单击“属性”→“高级”→“WINS”命令，选中“禁用 TCP/IP 上的 NetBIOS”选项，即可完成任务，如图 2.6 所示。

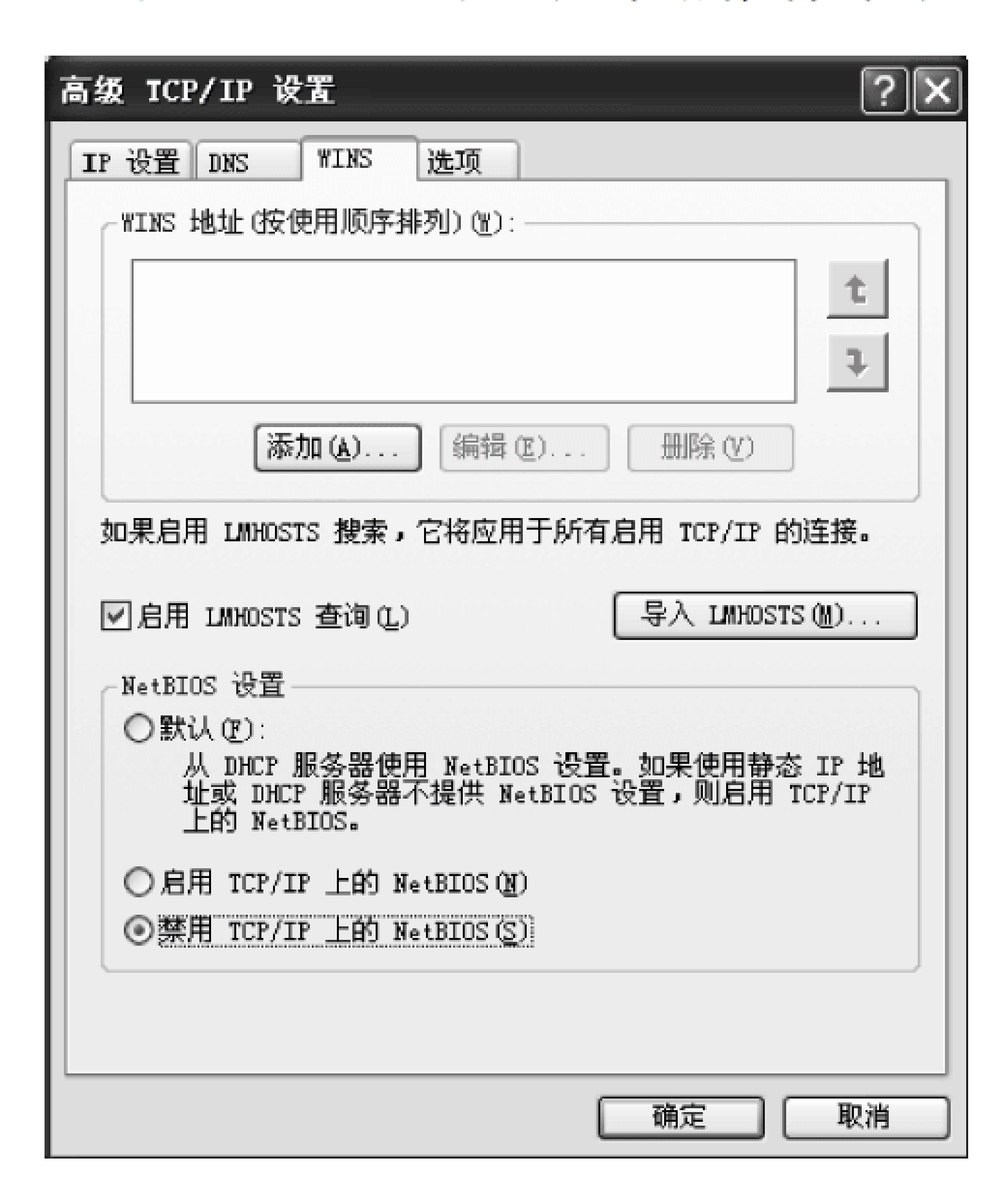


图 2.6　禁用 TCP/IP 上的 NetBIOS

② 通过注册表关闭 445 端口

445 端口是一把“双刃剑”，有了它用户可以在局域网中轻松访问各种共享文件夹或共享打印机，但也正是因为有了它，黑客们才有了可乘之机。它们可通过该端口偷偷共享用户的硬盘，甚至会在悄无声息中将用户的硬盘格式化掉。用户要做的就是想办法不让黑客有机可乘，封堵住 445 端口漏洞。

进入注册表，HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters，选择“Parameters”选项，右击，选择“新建”→“DWORD 值”，将 DWORD 值命名为“SMBDeviceEnabled”，数值为 0。

③ 关闭 3389 端口

3389 端口是 Windows 2000/2003 远程桌面的服务端口，可以通过这个端口用“远程桌面”等工具来连接到远程服务器。如果连接上远程服务器，输入系统管理员的用户名和密码后就会像操作本机一样操作远程计算机，因此远程服务器一般都将该端口修改数值或者关闭。关闭 3389 端口的过程如下：

如果是 Windows 2000 Server 系统，单击“开始”→“程序”→“管理工具”命令，选择 Terminal Services 服务项，单击“属性”项将启动类型改成“手动”，并停止该服务即可。

如果是 Windows XP 系统，右击“我的电脑”，选择 “属性”选项，单击“远程”，将里面的“远程协助”和“远程桌面”两个选项框里的“√”去掉即可，如图 2.7 所示。

④ 关闭 4899 端口

4899 是一个远程控制软件所开启的服务端端口，由于这些控制软件功能强大，所以经常被黑客用来控制自己的“肉鸡”。而且这类软件一般不会被杀毒软件查杀，对黑客来说，它

比后门还要安全。4899 不像 3389 那样，是系统自带的服务。需要自己安装，而且需要将服务端上传到入侵的计算机并运行服务，才能达到控制的目的。所以只要对用户计算机进行了基本安全配置，黑客是很难通过 4899 来控制用户的。

具体操作为：单击“开始”→“设置”→“网络连接”→“本地连接”→“属性”→“Internet 协议(TCP/IP)”→“属性”→“高级”→“选项”→“TCP/IP 筛选”→“属性”命令，打开“TCP/IP 筛选”对话框，添加需要的 TCP、UDP 协议即可，如图 2.8 所示。

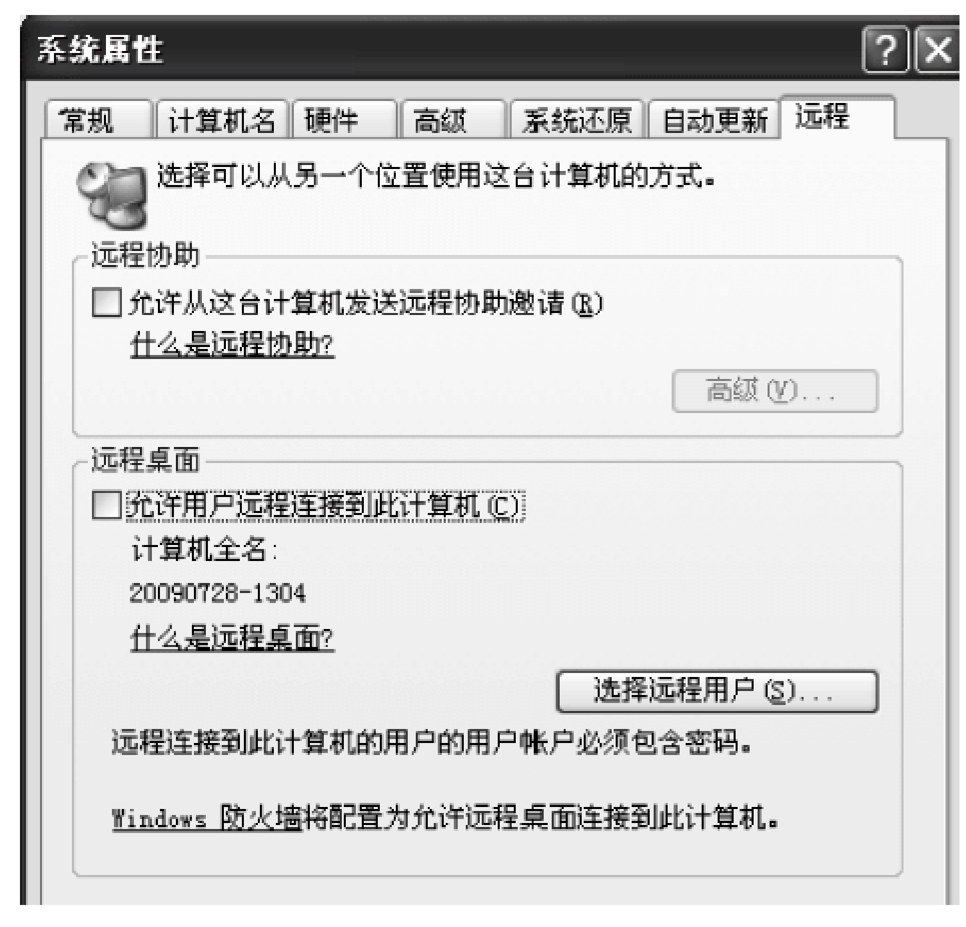



图 2.7 Windows XP 系统的“远程”窗口



图 2.8 “TCP/IP 筛选”对话框

(5) 关闭无用的服务

对于个人用户来说，系统安装过程中默认的有些端口是没有什么用途的，应该关掉这些端口，即关闭无用的服务。管理员还可以把系统中不必要的服务都禁止掉，尽管这些不一定能被攻击者利用得上，但是按照安全规则和标准看，多余的东西就没必要开启，这样还可减少一些隐患。对于个人用户，可关闭如下不常用的服务：

- Alerter：警报器，通知所选用户和计算机有关系统管理级警报。
- ClipBook：启用“剪贴簿查看器”储存信息并与远程计算机共享服务。
- Computer Browser：维护网络上计算机的最新列表及提供这个列表。
- Distributed File System：局域网管理共享文件。
- Distributed Linktracking Client：用于局域网更新连接信息。
- Error Reporting Service：发送错误报告。
- Help and Support：帮助和支持服务。
- Indexing Service：索引服务。
- Messenger：传输客户端和服务器之间的 NET SEND 和警报器服务消息。
- Microsoft Search：提供快速的单词搜索。
- Network DDE：网络动态数据交换。
- PrintSpooler：如果没有打印机可禁用。
- QoS RSVP：服务质量资源预留服务。
- Remote Registry：远程修改注册表。

- Remote Desktop Help Session Manager：远程协助。
- Task scheduler：允许程序在指定时间运行。

关闭不常用服务的操作如下：

单击“开始”→“程序”→“管理工具”→“服务”命令，打开“服务”窗口，窗口中显示了很多服务（包括服务名称、服务状态、服务描述和启动类型等），如图 2.9 所示。选定要关闭的服务名称并双击，弹出如图 2.10 所示的对话框。将启动类型改为“已禁用”。单击“停止”按钮，将服务状态改变为“已停止”，再单击“确定”按钮，完成禁止该服务设置。

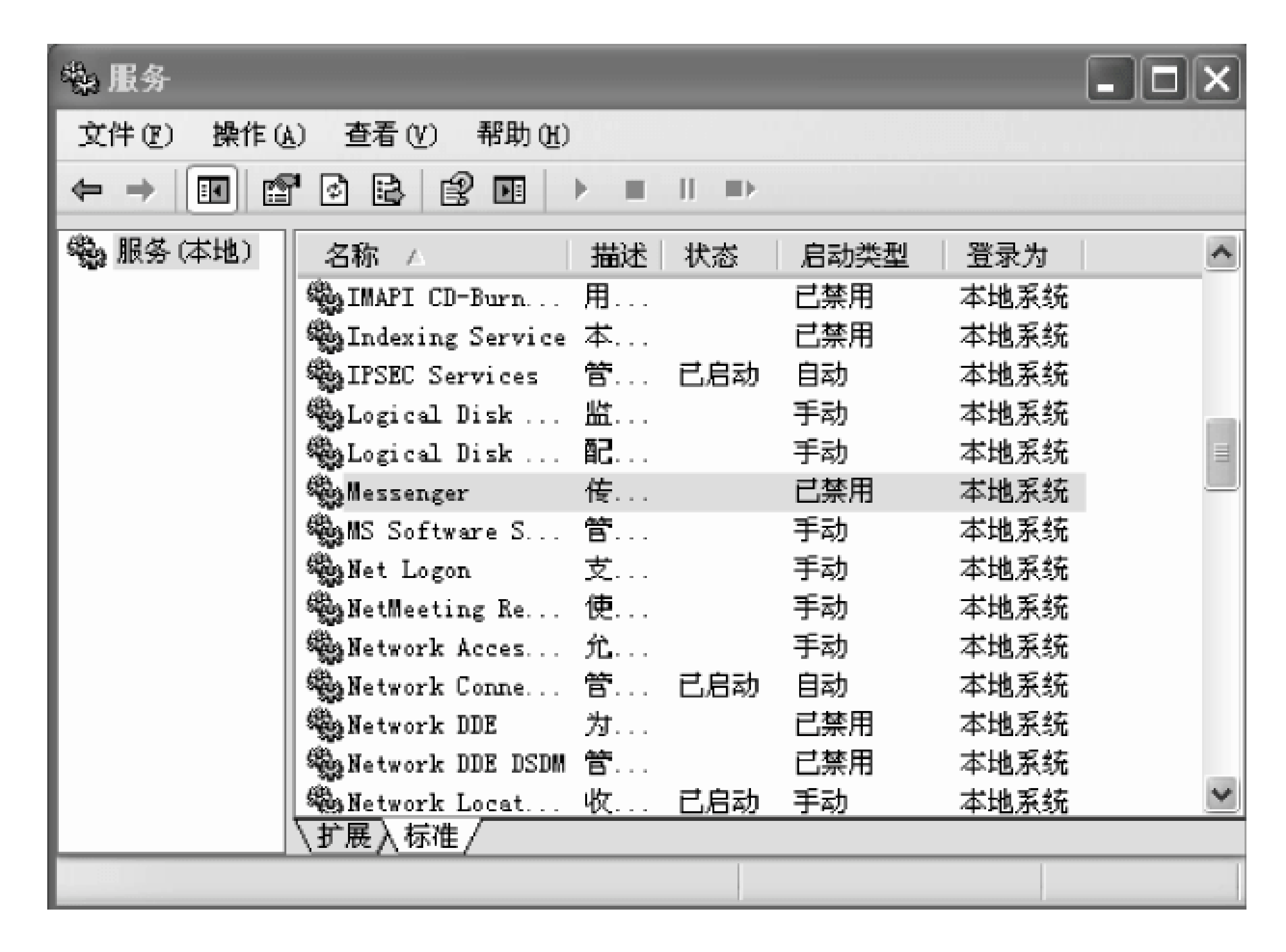


图 2.9 “服务”窗口



图 2.10 禁止服务窗口

再依次选择不用的服务，按上述步骤关闭即可。这样在下次重启服务后已进行关闭设置的服务就被禁止了。

(6) 目录和文件权限管理

为了控制好服务器上用户的权限,同时也为了预防以后可能的入侵和溢出,必须精心地设置目录和文件的访问权限。Windows 的访问权限一般分为读取、写入、读取及执行、修改、列目录和完全控制。在默认情况下,大多数文件夹对所有用户(Everyone 组)是完全控制的(FullControl),用户可根据应用的需要进行权限重设。

可以采用如下措施来管理目录和文件的权限。

- 将 C 盘的所有子目录和子文件继承 C 盘的 Administrator(组或用户)和 SYSTEM 目录具有的全部权限。
- 修改 C:\ProgramFiles\CommonFiles,开放 Everyone 默认的读取及运行,列出文件目录和读取权限。
- 开放 Everyone 的修改、读取及运行,列出文件目录,读取和写入权限。
- 为防止非法访问,可将 cmd.exe 和 net.exe 两个文件的权限修改为特定管理员才能访问,如:

```
cmd.exe root 用户所有权限
net.exe root 用户所有权限
```

- 使用 comlog 程序将 com.exe 改名为_com.exe,然后替换 com 文件(可以记录所有执行的命令行指令)。

(7) 不使系统显示上次登录的用户名

默认情况下,终端服务接入服务器时,登录对话框中会显示上次登录的账户名,本地的登录对话框也是一样。这使得别人可以很容易地得到系统的一些用户名,进而可进行密码猜测。修改注册表可以不使对话框显示上次登录的用户名。具体操作过程是:

单击"开始"→"运行"命令,输入 regedit,确认后进入注册表,HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Dont DisplayLastUserName,把 REG_SZ 的键值改成 1。

(8) 把敏感文件存放在另外的文件服务器中

虽然现在服务器的硬盘容量都很大,但为了安全起见,还应考虑把一些重要的用户数据(文件、数据表、项目文件等)存放在另外一个服务器中,并且经常备份它们。

(9) NTFS 分区安全

① 使用 NTFS 格式分区

把服务器的所有分区都改成 NTFS 格式。NTFS 文件系统要比 FAT、FAT32 的文件系统安全得多。

② 用 NTFS 数据流给文件加密

Windows XP 用户可利用 NTFS 数据流来给文件或文件夹加密。由于 FAT32 文件系统格式不支持数据流格式,所以必须在 NTFS 文件系统下才能实现本次加密。如果硬盘分区格式不是 NTFS,可以在命令模式下用

```
converntc <盘符:>/FS:NTFS
```

命令进行转换。

第 1 步:在要加密的文件或文件夹(如 abc)图标上右击,单击"属性"命令打开文件夹属

性对话框。在“常规”选项中单击“高级”按钮，如图 2.11 所示，打开“高级属性”对话框。

第 2 步：在该对话框的“压缩或加密属性”选项区域中选择“加密内容以便保护数据”复选框，然后单击“确定”按钮，即可完成文件或文件夹的加密，如图 2.12 所示。此时再打开该文件或文件夹，文件或文件夹的内容都已经被隐藏了。



图 2.11　文件夹“属性”对话框

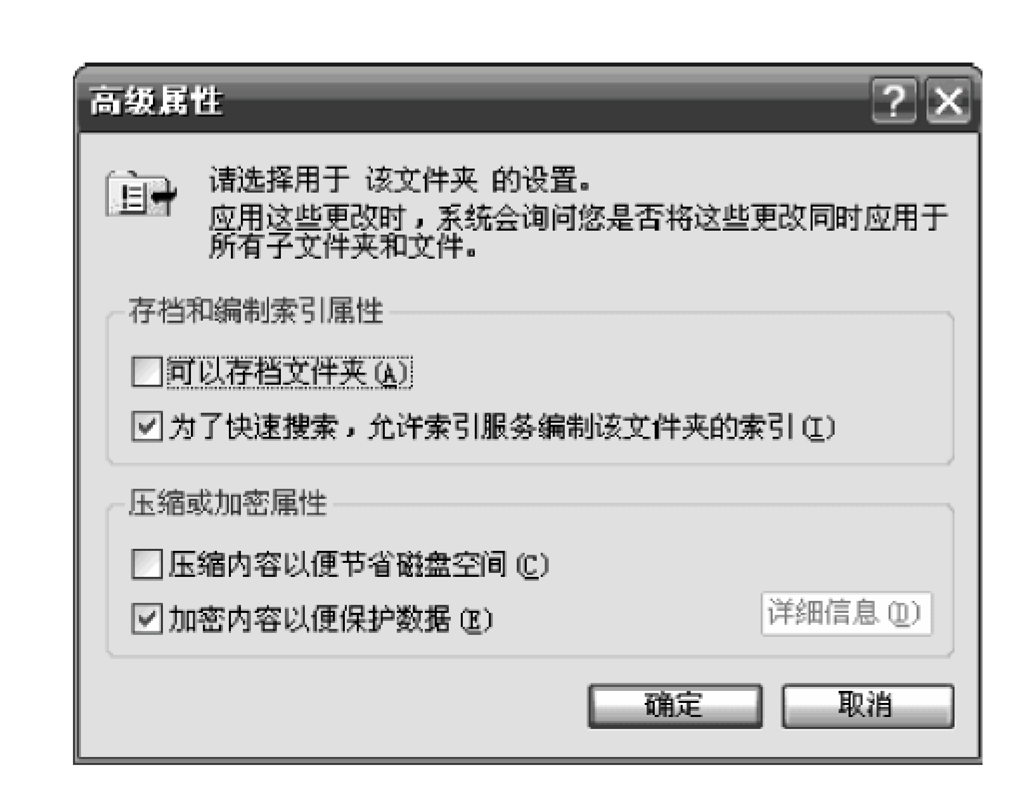


图 2.12　文件或文件夹的加密

(10) 服务器日常管理

① 服务器的定时重启(如每台服务器保证每周重新启动一次，重新启动之后要进行复查，确认服务器已经启动了，确认服务器上的各项服务均恢复正常)。

② 服务器的安全、性能检查(如每台服务器至少保证每周登录两次、简单检查两次，并将每次检查的结果进行记录)。

③ 服务器的数据备份(如每台服务器至少保证每月备份一次系统数据，每两周备份一次应用程序数据，每月备份一次用户数据等)。

④ 服务器的监控(如每天正常工作期间必须保证监视所有服务器状态，一旦发现服务停止要及时采取相应措施)。

⑤ 服务器的相关日志操作(如每台服务器保证每月对相关日志进行一次清理，清理前对应的各项日志如应用程序日志、安全日志、系统日志等都应选择“保存日志”)。

⑥ 服务器的补丁修补和应用程序更新(如使用新出的漏洞补丁，在第一时间给每台服务器打上补丁进行应用程序方面的安全更新)。

⑦ 服务器的隐患检查(包括安全隐患、性能等方面的检查，每台服务器必须保证每月重点单独检查一次，每次检查结果必须做好记录)。

⑧ 定期管理密码更改(如每台服务器保证至少每一个月或两个月更改一次密码)。

除上述服务器安全措施外，还有一些其他安全手段，可以有选择地为服务器设置，如安全日志、SQL Server 数据库服务器安全、设置 IP 筛选、禁止木马常用端口等。

2.5 客户机安全

在企业、单位的内部网络中，除了一些提供网络服务的服务器外，应用更多的是客户机（工作站）或可移动的笔记本电脑。网络管理人员可以考虑制定标准的客户机安全政策，利用一些安全设定与保护机制来管理这些有潜在风险的客户机。

客户机是对企业网络进行内部攻击的最常见的攻击源，构成了对系统安全管理员的挑战。一是因为网络中客户机的数量最多，二是因为许多用户没有接受过网络安全教育，或者不关心网络安全问题。虽然阻止外部对网络内部客户机进行访问相对容易，但要防止内部的攻击就困难得多，无论这种攻击是否是有意的。

与网络的其他部分一样，实现客户机安全的最佳途径很多。可限制用户对网络的访问权限，限制用户更改机器配置的能力，在每一台客户机上运行防病毒软件并经常更新病毒定义。通过对客户机安全施加严格的限制，可以使许多安全问题在发生之前避免。

2.5.1 客户机的安全策略

1. 客户机实体安全

（1）设定使用者授权机制

在企业、单位内部网络环境里，可以明确唯有授权的使用者方可使用内部网的工作站主机。另外，使用者可以启动屏幕保护程序来限制未被授权的人使用，以保护工作站中所存放的数据。

（2）设定访问控制权限

对于客户机中机密或重要的档案/目录进行权限控制，非授权人无法读取重要的文件或利用密码保护功能进行控制。

（3）定期执行备份工作

工作站上重要的档案需定期备份，或者将档案备份到内部网络的档案伺服主机上。

2. 客户机系统安全设定

（1）重视软件相关的安全修补程序

注意软件开发厂商提供的修补程序，并确实执行修补作业。

（2）安装防毒软件并定期更新病毒码

利用防毒软件进行病毒的防护机制，并确实更新程序，以达到有效的预防。

（3）远程管理的安全性

远程管理工具提供给 IT 人员一个便利的管道来管理企业中的计算机，但可能一不小心便成为黑客的后门，IT 人员需特别注意。

（4）减少不必要的应用程序

在工作站上只要有不必要的应用程序，就将它移除或停止启动。

（5）合理使用客户机管理程序

网络管理人员可以合理使用客户机管理程序来管理内部网络的软硬件，找出是否有工

作站安装了未经授权的软件,或执行了不安全的软件。

(6) 不随意下载或执行来源不明的文档或程序

网络管理人员要提醒每个使用者不要执行来路不明的程序,减少信息安全的风险。

2.5.2 客户机的安全管理与应用

1. 客户机物理安全

物理安全涉及对计算机的访问。提到物理安全时要考虑两方面的问题:一是客户机整机被窃;二是未授权人员通过客户机获得对网络的访问权。

笔记本电脑特别易于产生第一类问题,因为用户经常会把笔记本电脑整夜放在单位、私车或其他很容易被偷盗的场所。但台式机系统的安全性也应引起注意,因为一般人不可能偷走整台客户机,但有特殊目的的人或公司间谍却会这样做。

所有的台式机应该固定到桌子上,或者固定在更为安全的地方。这虽然不会阻挡那些有目的偷窃某台特殊台式机的人员,但是它会降低台式机对一般盗窃人员的吸引力。

确保把文件存储在文件服务器中而不是存储在本地硬盘中,客户机和笔记本电脑的安全性也因此而增强。这样使备份工作也更易于实行,也意味着即使某个人偷窃了客户机,机器上也基本上没有有价值的文档。

常见的发生非授权用户通过客户机获得对网络的访问权原因,是用户没有锁定自己的客户机。因为网络操作系统允许用户在离开时锁定计算机,这时用户不需要关闭机器,也不需要退出网络。用户只在离开客户机时使用锁定功能即可容易地防止其他人再使用这台客户机。许多操作系统也允许客户机在空闲一定时间后自动进入锁定模式。

2. 管理员访问权限

管理员账号通常是指 Windows 系统中的 Administrator 或 UNIX 系统中的 root。该账号对于系统中的任何程序和文件具有完全的访问和管理权。管理员可以对系统配置进行全局修改,能够增加和删除其他系统账号。

当网络用户以用户账号登录到客户机时,用户可通过远程服务器进行验证。通常用户也可在客户机上创建本地账号。这个账号允许用户在不连接到网络的情况下登录客户机。网络上的每一个用户都有一个配置文件,也可是多个用户具有相同的配置文件,这些用户通常属于同一个工作组。

系统管理员能够限制用户和工作组可用的访问权限类型,也可以选择限制会计工作组账号,以使它的成员只能访问会计文件服务器并且会计工作组的成员不能在他们的机器上安装任何软件。

通过分组的方式管理安全访问权限比通过管理单个用户的方式更加容易,这也是多数管理员选择使用的原因。分配特定权限和特权给工作组允许管理员控制网络数据流量,有助于防止对网络设备的非授权访问。

控制安装在客户机上的应用程序类型也是非常重要的。除具有管理权限的用户可以安装应用程序外,不允许其他用户安装任何程序。如果某些用户需要能够定期地安装测试软件,则可赋予这些用户对自己所用客户机的管理员权限,也可以创建一个实验环境,在实验

环境下，用户可以测试和安装软件，即给予他们有限的安装软件的权限。

3. 远程登录

用户不应该从网络外部对他们的机器进行远程访问。在客户机上应该禁用所有的远程访问软件。防火墙规则可以防止远程用户尝试访问客户机，但是不能阻止他们在网络内部使用这些工具。为了防止这种情况，应该建立合适的安全审计系统。

完全关闭对客户机的远程访问是不必要的，也不建议这样做。管理人员经常需要访问客户机，以检查问题或者安装新软件。多数网络操作系统有内建的管理此类任务的工具，应该使用这些工具来完成。

与其他方面一样，在使用远程登录服务管理机器之前，确保已经分析了所有的安全风险。当利用台式机用户远程登录时，如果攻击者能够嗅探到管理员访问客户机的口令，就需要考虑采用另一种远程访问方法。无论管理员选择使用哪种类型的远程访问系统，在管理员和客户机之间传送的所有信息都应合理地进行加密，这一点很重要。

4. 客户机安全设置

在使用服务器 Internet 连接共享的网络中，黑客不能直接攻击到客户机，最多只能对主机造成威胁。如在客户机上使用 QQ 即时通信软件时，有人在 Internet 上测得的 IP，其实是服务器的 IP，因此服务器因被发现而受到攻击，而客户机却没被发现。下面介绍的是两种简单的客户机安全设置实践。

(1) 配合使用服务器的 DHCP 功能

在服务器上使用 DHCP 功能后，可以更好地保证局域网中每台客户机的安全性，但客户机也必须配合使用，否则会出现局域网 IP 冲突，或无故断线等怪现象。设置方法很简单，在 TCP/IP 属性里面选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”就可以了，如图 2.13 所示。

(2) 合理使用代理

有效合理地使用 Internet 上提供的代理服务器可以提高客户机的安全系数。客户机通过局域网服务器与互联网上的代理服务器连接，并通过代理服务器实现不同的网络方式，即使黑客查找到网络信息也只是代理服务器的信息，这样虽不是 100%的安全，但是提高了整个网络的安全性。使用代理服务器会提高客户机的安全系数，但却以牺牲性能为代价，所以是否使用该方法应酌情而定。

代理设置的具体操作步骤如下：

第 1 步：对 HTTP、FTP 等网络方式设置代理时，打开控制面板中的“Internet 选项”，弹出“Internet 属性”窗口，打开“连接”选项卡，如图 2.14 所示。

第 2 步：单击图 2.14 右下侧的“局域网设置”按钮，在“局域网(LAN)设置”里将“为 LAN 使用代理服务器”复选框选中，如图 2.15 所示。

第 3 步：单击“高级”按钮，弹出如图 2.16 所示的“代理服务器设置”对话框，可填写详细的代理信息。

第 4 步：设置完毕，单击“确定”按钮，完成代理设置。



图 2.13　TCP/IP 属性



图 2.14　Internet 属性——连接

图 2.15　局域网设置



图 2.16　“代理服务器设置”对话框

5. 台式机和笔记本电脑的区别管理

系统管理员面临的一个常见问题是决定使用台式机还是笔记本电脑。台式机不易移动，易于管理。当系统管理员需要访问台式机时，马上就可以做到。但现在使用笔记本电脑的用户很多，特别是那些经常外出或者在家里做大量工作的用户。由于笔记本电脑功能变得越来越强大，它们在公司环境中正慢慢取代台式机。雇员需要远程工作，他们就可在家里上网，不需要在家用计算机上安装特殊的软件。

虽然笔记本电脑的好处很明显，但是它们很容易出现管理和安全方面的问题。在家中和工作中使用笔记本电脑的雇员会把它作为自己的物品来对待，电脑上可能安装了未经批

准的软件或者操作系统，这些软件也可能是未经许可的，这会使笔记本电脑存在受攻击的可能。

此外，笔记本电脑也应做备份。当预先安排执行的备份工作开始时，如果笔记本电脑没有连接在网络上，这项工作就不能完成。文件服务器对于笔记本电脑用户更加重要，在可能的情况下，用户应该把文件手工复制到文件服务器中。

因此，管理员要制定有关安全措施，对使用笔记本电脑的用户进行严格管理和要求。在发放笔记本电脑时必须对所有用户解释清楚保持笔记本电脑完整的重要性。

习题和思考题

一、问答题

1. 解释网络冗余安全中的“冗余”含义及冗余的目的。
2. 简述路由选择算法及其分类。
3. 简述路由器访问控制的安全策略。
4. 简述安全交换机的新功能。
5. 简述服务器的安全策略。
6. 简述客户机实体安全和系统安全策略。
7. 列举几种网络上常用的服务器。

二、填空题

1. 常用的网络硬件设备包括客户端硬件设备(如　　)和网络设备(如　　)两大类。
2. “冗余”就是(　　)，以保证系统更加可靠、安全地工作。
3. 网络系统的主要设备有(　　)、(　　)、(　　)以及网络边界设备等。
4. (　　)是网络的神经中枢，是众多网络设备的重要一员，它担负着网间互连、路由走向、协议配置和网络安全等重任，是信息出入网络的必经之路。
5. 路由选择算法可分为(　　)路由选择算法和(　　)路由选择算法两大类。
6. (　　)是一种基于 MAC(网卡的硬件地址)识别，能完成封装转发数据包功能的网络设备，它在内部网中占有重要的地位，通常是整个网络的核心所在。
7. 安全交换机具有(　　)、(　　)和入侵检测系统等功能。
8. 按照服务用途，网络服务器有(　　)、(　　)、(　　)和电子邮件服务器等。

三、实验题

1. 在 Cisco 路由器上进行 RIP 路由协议配置。
2. 禁止路由器部分网络服务的配置。
3. Cisco 交换机口令的安全配置。
4. 对交换机进行配置使 IP 地址与 MAC 地址绑定。

第3章 网络操作系统安全与管理实践

网络系统是由多个相互独立的计算机系统通过通信媒体连接起来的。各计算机都具有一个完整独立的操作系统,网络操作系统(network operating system,NOS)是建立在这些独立的操作系统基础上的、用以扩充网络功能的系统。网络操作系统是网络的心脏和灵魂,是向网络计算机提供服务的特殊的操作系统。它在计算机操作系统下工作,使计算机操作系统增加了网络操作所需要的能力。网络操作系统运行在称为服务器的计算机上,并由联网的计算机用户共享,这类用户称为客户。

3.1 常用网络操作系统简介

网络操作系统是为使网络用户能方便而有效地共享网络资源而提供各种服务的软件及相关规程的集合,是网络软件系统的基础。它是整个网络的核心,通过对网络资源的管理,为用户方便而有效地使用网络资源提供网络接口和网络服务。网络操作系统除了具有一般的操作系统所具有的处理机管理、存储器管理、设备管理和文件管理功能外,还提供高效而可靠的网络通信环境和多种网络服务功能。

常用的网络操作系统有 Microsoft 公司的 Windows NT、Windows 2000 Server、Windows Server 2003 和 Windows XP,Novell 公司的 NetWare,SCO 公司的 UNIX 和 RedHat 公司的 Linux。Windows 2000 是在 Windows NT 基础上,在安全性、可操作性等方面都做了较大的改进后,由 Microsoft 公司推出的网络操作系统,为广大用户所接受。Windows Server 2003 则是依据.NET 架构对 Windows NT 技术进行了重要发展和实质性改进的一种全新的操作系统。大多数网络都是采用这几种网络操作系统构造的。

3.1.1 Windows NT

Windows NT 是 Microsoft 公司在 LAN Manager 网络操作系统基础上于 1993 年推出的具有更高性能的 NOS。在 Windows NT 问世的几年内,网络操作系统一直由 NetWare 垄断的局面被打破了,尤其在视窗环境下的用户界面、方便灵活的系统管理,使得越来越多的计算机用户转向 Windows NT 系统。

Windows NT 是一种 32 位多用户、多任务的网络操作系统,也是一种面向分布式图形应用程序的完整的平台系统。Windows NT 既可作为局域网络的服务器系统,为局域网上客户机提供多种服务,又可作为局域网上的客户系统,访问网上任何服务器。Windows NT

为网络管理提供了完善的解决方案；具备担负大型项目需求的能力；提供了健全的安全保护能力和具有独特的支持多平台的优势等。

Windows NT 网络软件主要包括 Windows NT Server(Windows NTS)和 Windows NT Workstation(Windows NTWS)两种。这两种版本都是 32 位操作系统，网络功能也都很完善。前者主要用于网络上的服务器，包括文件服务器、打印服务器和 Windows NT 网络的主域控制器等；后者则主要服务于高档客户。从网络角度看，Windows NTS 属于管理网络的主服务器软件，而 Windows NTWS 则用于管理特殊工作站或用户工作站。两者相比，服务器软件附带有较强的管理功能和较完善的 Internet 功能，如可以使用附带的 IIS 软件建立企业网的 Internet 信息服务器，而工作站软件只有较简单的单一 Web 服务功能。

Windows NT 是功能强大的网络操作系统，既适合于大型业务机构的实时、分时数据处理，又能为工作组、商业和企业的不同机构提供一种优化的文件和打印服务，其 Client/Server(C/S)平台还可以集成各种新技术，通过该平台为信息存取提供优越的环境。

Windows NT 操作系统在其核心内置了容错技术，可以在应用软件和系统硬件故障时，保证系统能正常可靠地工作；提供了相当多的易于实施的网络管理及网络安全功能，如创建用户组和用户，用户入网安全限制，进行各种 CPU 和内存的测试与分析等。

虽然工作站软件也可以被安装在计算机上作为服务器使用，但由于受其先天设计思想的限制，使多数服务器版本的软件无法在该环境中使用，因此在多数场合中不适宜作服务器使用。然而，对于那些希望享受操作系统比 Windows 95 更稳定、更安全的用户来说，使用 Windows NTWS 作为自己桌面的操作系统，可能是一个最佳选择。

Windows NT 系统涉及一些基本概念，如域(domain)、工作组(workgroup)、目录数据库、委托关系(trust relationships)等。

Windows NT 系统的服务有目录服务、文件共享服务、共享打印服务、网络互连服务、远程通信服务和 Internet 服务等，系统的 Web 服务器、FTP 服务器、DHCP(主机动态配置协议)服务器、WINS 服务器、DNS 服务器和邮件服务器等都可为用户提供相应的 Internet 服务。

3.1.2 Windows 2000/2003

1. Windows 2000 系统

在 Windows NT 之后，Microsoft 公司又推出了 Windows 2000 网络操作系统。与 Windows NT 相比，Windows 2000 在许多方面都做了较大的改进。在安全性、可操作性等方面都有了质的飞跃。

Windows 2000 系列操作系统有 Windows 2000 Datacenter Server、Windows 2000 Advanced Server、Windows 2000 Server 和 Windows 2000 Professional 版本。Windows 2000 Datacenter Server 是一个新的品种，它支持 32 个以上的 CPU 和 64GB 的内存，以及 4 个节点的集群服务。Windows 2000 Server 和 Advanced Server 分别是 Windows NT Server 4.0 及其企业版的升级产品。Windows 2000 Professional 是一个商业用户的桌面操作系统，也适合移动用户，是 Windows NT Workstation 4.0 的升级产品。

Windows 2000 系列操作平台继承了 Windows NT 的高性能，融入了 Windows 9x 易操

作的特点，又发展了一些新的特性。Windows 2000 使用了活动目录、分布式文件系统、智能镜像、管理咨询等新技术，具备了强大的网络功能，可作为各种网络的操作平台，尤其是Windows 2000 强化的网络通信，提供了强大的 Internet 功能，为搭建电子商务解决方案提供了可靠的、高性能的基础平台。

2. Windows 2003 系统

在微软的企业级操作系统中，如果说 Windows 2000 全面继承了 NT 技术，那么Windows Server 2003 则是依据.NET 架构对 NT 技术进行了重要发展和实质性改进，并部分实现了.NET 战略，构筑了.NET 战略中最基础的一环。Windows Server 2003 作为.NET 架构提出以来最重要、最基础性的产品，它的推出受到了业内人士的关注。

Windows Server 2003 是一款微软推出的全新操作系统。Windows Server 2003 简体中文版分 Web、Standard、Enterprise 和 Datacenter 四个版本。Enterprise 版最大支持 8 个处理器和 32GB 内存，最小配置为 CPU 速度不低 133MHz，内存不少于 128MB。因此，Windows Server 2003 具有硬件适应性面广和伸缩性强的特点。

Windows Server 2003 不仅改进了 Windows 2000 原有的服务，提高了这些服务的性能和扩充了许多功能，而且还增加了新的服务。如安全性、可管理性和系统性能等。Windows Server 2003 改进并增强了远程控制功能、Net Framework 计算平台、IIS 6.0、流媒体服务和关闭事件跟踪功能等。

从安全性角度看，原来的 Windows 系统的安全性总是不尽如人意，直到 Windows 2000 才有较大改观，但依然存在缺憾，如登录时的输入法漏洞、IIS 特殊网址漏洞等。Windows Server 2003 在安全上下了大工夫，不仅堵住了已发现的 NT 漏洞，而且还重新设计了安全子系统，增加了新的安全认证，改进了安全算法。

在本地安全策略方面，Windows 2003 区别于 Windows 2000 之处在于软件限制策略(SRP)。Windows 2003 的 SRP 允许用户控制在本地计算机系统上运行哪些软件。用户可在选项中规定系统要运行的软件，因此可阻止不被信任的软件运行。用户可定义默认的安全级别为 Unrestricted(允许未明确拒绝的)或 Disallowed(拒绝未明确允许的)。后者有较好的安全级别，但限制过于严格。

在用户组策略方面，Windows 2003 系统在组策略中增加了两项内容：软件限制策略(SRP)和无线网络策略(IEEE 802.11)。软件限制策略的功能与本地安全策略相同，但它可应用到站点、域或机构单位(OU)。无线网络策略允许管理员管理无线网络，定义优先的无线网络，并对任何系统定义 802.1x 身份验证。

Windows 2003 的安全中心是活动目录(AD)。它集成了最新版本的 Windows 操作系统中的目录服务。Windows 2003 的活动目录比 Windows 2000 的活动目录的灵活性和可管理性更强，可以处理森林域信任关系。

3.1.3　Linux 和 UNIX

1. Linux 系统

Linux 是一种类似 UNIX 操作系统的自由软件，它是由芬兰赫尔辛基大学的一位叫

Linus 的大学生发明的。1991 年 8 月，Linus 在 Internet 上公布了他开发的 Linux 的源代码。由于 Linux 具有结构清晰、功能简捷和完全开放等特点，许多大学生和科研机构的研究人员纷纷将其作为学习和研究对象。他们在修改原 Linux 版本中错误的同时，也不断为 Linux 增加新的功能。在全世界众多热心者的努力下，Linux 操作系统得以迅速发展，成为一个稳定可靠、功能完善的操作系统，并赢得了许多公司的支持，包括提供技术支持。开发 Linux 应用软件，并将其应用推广，这也大大加快了 Linux 系统商业化的进程。国际上许多著名 IT 厂商和软件商纷纷宣布支持 Linux。Linux 很快被移植到 Alpha、PowerPC、Mips 和 Sparc 等平台上，从 Netscape、IBM、Oracle、Informix 到 Sybase 均已推出 Linux 产品。Netscape 对 Linux 的支持，大大加强了 Linux 在 Internet 应用领域中的竞争地位。大型数据库软件公司对 Linux 的支持，则为其进入大中型企业的信息系统建设和应用领域奠定了基础。

在中国，随着 Internet 的发展和网民的迅速增加，一支主要由高校学生和 ISP 技术人员组成的 Linux 爱好者队伍已蓬勃发展起来，曾兴起"Linux 热"。随后 Linux 在国内得到了大规模的应用和普及。可以说，随着 Internet 的普及应用，免费而性能优异的 Linux 操作系统将发挥越来越大的作用。

Linux 之所以发展得如此之快，不能不说是 Internet 的功劳，因为对 Linux 的讨论和研究都是通过 Internet 进行的。Linux 和 Internet 的发展相辅相成，没有 Internet，就没有 Linux 的诞生和发展。反过来，Linux 的发展也大大促进了 Internet 的发展，因为 Linux 是一个完全公开的操作系统，每个人都可以得到它的源代码，这使得许多人的才能有了用武之地。在 Internet 上，自学成为 Linux 专家已成为年轻人的最大梦想之一。

Linux 继承了 UNIX 的很多优点(如多任务、多用户)，还具有共享内存页面、使用分页技术的虚拟内存、动态链接共享库、支持多个虚拟控制台、调度磁盘缓冲功能、支持多平台、与其他 UNIX 系统兼容、提供全部源代码及支持多种 CPU、多种硬件、软件移植性好等特点。

2. UNIX 系统

1970 年，在美国电报电话公司(AT&T)的贝尔(Bell)实验室研制出了一种新的计算机操作系统，这就是 UNIX。UNIX 是一种分时操作系统，主要用在大型机、超级小型机、RISC 计算机和高档微机上。在整个 20 世纪 70 年代它得到了广泛的普及和发展。许多工作站生产厂家使用 UNIX 作为其工作站的操作系统。在 20 世纪 80 年代，由于世界上各大公司纷纷开发并形成自己的 UNIX 版本，出现了分裂局面，加之受到了 NetWare 的极大冲击，UNIX 曾一度衰败。20 世纪 90 年代，开发和使用 UNIX 的各大公司再次加强了合作和对 UNIX 的统一进程，并加强了 UNIX 系统网络功能的深入研究，不断推出功能更强大的新版本，并以此拓展全球网络市场。20 世纪 90 年代中期，UNIX 作为一种成熟、可靠、功能强大的操作系统平台，特别是对 TCP/IP 的支持以及大量的应用系统，使得它继续拥有相当规模的市场，并保持了连续数年两位数字的增长。

UNIX 系统的再次成功取决于它将 TCP/IP 协议运行于 UNIX 操作系统上，使之成为 UNIX 操作系统的核心，从而构成了 UNIX 网络操作系统。UNIX 操作系统在各种机器上都得到了广泛的应用，它已成为最流行的网络操作系统之一和事实上标准的网络操作系统。

UNIX 系统服务器可以与 Windows 及 DOS 工作站通过 TCP/IP 协议连接成网络。UNIX 服务器具有支持网络文件系统服务、提供数据库应用等优点。

UNIX 系统是一个可供多用户同时操作的会话式分时操作系统。不同的用户可以在不同的终端上,通过会话方式控制系统操作。UNIX 系统继承了以往操作系统的先进技术,又在总体设计思想上有所创新。在操作系统功能设计上力求简捷、高效。UNIX 系统向用户提供了两种界面:一种是用户使用命令,通过终端与系统进行交互的界面,即用户界面;另一种是用于用户程序与系统的接口,即系统调用。UNIX 系统采用树型结构的文件系统,由基本文件系统和可装卸的若干个子文件系统组成,既能扩大文件存储空间,又具有良好的安全性、保密性和可维护性。UNIX 系统是能在笔记本电脑、PC、工作站、中小型机乃至巨型机上运行的操作系统。因此,UNIX 系统具有极强的可伸缩性。

3.2　网络操作系统安全与管理

网络操作系统在网络应用中发挥着十分重要的作用。因此,网络操作系统本身的安全就成为网络安全保护中的重要内容。

操作系统主要的安全功能包括存储器保护(限定存储区和地址重定位,保护存储信息)、文件保护(保护用户和系统文件,防止非授权用户访问)、访问控制、身份认证(识别请求访问的用户权限和身份)等。

3.2.1　网络操作系统安全与访问控制

1. 网络操作系统安全

网络操作系统安全保护的研究,通常包括如下内容。

(1) 操作系统本身提供的安全功能和安全服务。现代操作系统本身往往要提供一定的访问控制、认证和授权等方面的安全服务。如何对操作系统本身的安全性能进行研究和开发,使之符合特定的环境和需求,是操作系统安全保护的一个方面。

(2) 针对各种常用的操作系统,进行相关配置,使之能正确对付和防御各种入侵。

(3) 保证网络操作系统本身所提供的网络服务能得到安全配置。

网络操作系统安全是整个网络系统安全的基础。操作系统安全机制主要包括访问控制和隔离控制。隔离控制主要有物理(设备或部件)隔离、时间隔离、逻辑隔离和加密隔离等实现方法;而访问控制是安全机制的关键,也是操作系统安全中最有效、最直接的安全措施。

访问控制系统一般包括主体、客体和安全访问政策。

(1) 主体(subject):主体是指发出访问操作、存取请求的主动方,它包括用户、用户组、主机、终端或应用进程等。主体可以访问客体。

(2) 客体(object):客体是指被调用的程序或要存取的数据访问,它包括文件、程序、内存、目录、队列、进程间报文、I/O 设备和物理介质等。

(3) 安全访问政策:安全访问政策是一套规则,可用于确定一个主体是否对客体拥有访问能力。

操作系统内的活动都可以看做是主体对计算机系统内部所有客体的一系列操作。操作

系统中任何含有数据的东西都是客体,可能是一个字节、字段或记录程序等。能访问或使用客体活动的实体是主体,主体一般是用户或者代表用户进行操作的进程。

在计算机系统中,对于给定的主体和客体,必须有一套严格的规则来确定一个主体是否被授权获得对客体的访问。

一般来说,如果一个计算机系统是安全的,即指该系统能通过特定的安全功能控制主体对客体信息的访问,也就是说只有经过授权的主体才能读、写、创建或删除客体信息。

2. 网络访问控制

(1) 访问控制的类型

为了系统信息的保密性和完整性,对网络系统需要实施访问控制。访问控制也称为授权,它是对用户访问网络系统资源进行的控制过程。只有被授予一定权限的用户,才有资格去访问有关的资源。访问控制具体包括两方面含义:一是指对用户进入系统的控制,最简单最常用的方法是用户账户和口令限制,其次还有一些身份验证措施;二是用户进入系统后对其所能访问的资源进行的限制,最常用的方法是访问权限和资源属性限制。

访问控制所考虑的是对主体访问客体的控制。主体一般是以用户为单位实施访问控制(划分用户组只是对相同访问权限用户的一种管理方法),此外,网络用户也有以 IP 地址为单位实施访问控制的。客体的访问控制范围可以是整个应用系统,包括网络系统、服务器系统、操作系统、数据库管理系统以及文件、数据库、数据库中的某个表甚至是某个记录或字段等。一般来说,对整个应用系统的访问,宏观上通常是采用身份鉴别的方法进行控制,而微观控制通常是指在操作系统、数据库管理系统中所提供的用户对文件或数据库表、记录/字段的访问所进行的控制。

访问控制可分为自主访问控制和强制访问控制两大类。

① 自主访问控制

所谓自主访问控制,是指由系统提供用户有权对自身所创建的访问对象(文件、数据表等)进行访问,并可将这些对象的访问权授予其他用户或从授予权限的用户处收回其访问权限。访问对象的创建者还有权进行“权限转让”,即将“授予其他用户访问权限”的权限转让给别的用户。需要指出的是,在一些系统中,往往是由系统管理员充当访问对象的创建者,并进行访问授权,而在其后通过“授权转让”将权限转让给指定用户。自主访问控制允许用户自行定义其所创建的数据,它以一个访问矩阵来表示包括读、写、执行、附加以及控制等访问模式。

② 强制访问控制

所谓强制访问控制,是指由系统(通过专门设置的系统安全员)对用户所创建的对象进行统一的强制性控制,按照规定的规则决定哪些用户可以对哪些对象进行何种操作系统类型的访问,即使是创建者用户,在创建一个对象后,也可能无权访问该对象。

强制访问控制策略以等级和范畴作为其主、客体的敏感标记。这样的等级和范畴,必须由专门设置的系统安全员,通过由系统提供的专门界面来进行设置和维护,敏感标记的改变意味着访问权限的改变。因此可以说,所有用户的访问权限完全是由安全员根据需要确定的。强制访问控制还有其他安全策略,如“角色授权管理”。该策略将系统中的访问操作按角色进行分组管理,一种角色执行一种操作,由系统安全员进行统一授权。当授予某一用户

某个角色时，该用户就有执行该角色所对应的一组操作的权限。当安全员撤销其授予用户的某一角色时，相应的操作权限也同时被撤销。

（2）访问控制措施

访问控制是保证网络系统安全的主要措施，也是维护网络系统安全、保护网络资源的重要手段。通常具体的访问控制措施有以下几种。

① 入网访问控制

入网访问控制是为用户安全访问网络设置的第一道关口。它是通过对某些条件的设置来控制用户是否能进入网络的一种安全控制方法。它能控制哪些用户可以登录网络，在什么时间、地点（站点）登录网络等。

入网访问控制主要就是对要进入系统的用户进行识别，并验证其合法身份。系统可以采用用户账户和口令、账户锁定、安全标识符及其他一些身份验证等方法实现。

每个用户在进行网络注册时，都要由系统指定或由用户自己选择一个用户账户（用户名）和用户口令。这些用户账户及口令信息都被存储于系统的用户信息数据库中。也就是说，每个要入网的合法用户都有一个系统认可的用户名和用户口令。

当用户要登录网络时，首先要输入自己的用户名和用户口令，然后服务器将验证用户输入的用户名和用户口令信息是否合法。如果验证通过，用户即可进入网络，去访问其所需要且有权访问的资源，否则用户将被拒于网络之外。

为了防止非法用户冒充合法用户尝试用穷举法猜测口令而登录系统，系统应为用户设定尝试登录的最大次数。在达到该次数数值后，系统将自动锁定该用户，不允许其再尝试登录。

必要时，系统为用户建立的账户中还可包含用户的入网时间、入网站点、入网次数和用户访问的资源容量等限制。

② 权限访问控制

一个用户登录入网后，并不意味着他能够访问网络中的所有资源。用户访问网络资源的能力将受到访问权限的限制。访问权限控制一个用户能访问哪些资源（目录和文件），以及对这些资源能进行哪些操作。

在系统为用户指定用户账户后，系统根据该用户在网络系统中要做的工作及相关要求，可为用户访问系统资源设定访问权限。用户要访问的系统资源包括目录、子目录、文件和设备；用户要对这些资源的访问操作可有读、写、建立、删除、更改等。

③ 属性访问控制

属性是文件、目录等资源的访问特性。系统可直接对目录、文件等资源规定其访问属性。通过设置资源属性可以控制用户对资源的访问。属性是在权限安全性的基础上提供的进一步的安全性。

属性是系统直接设置给资源的，它对所有用户都具有约束权。一旦目录、文件等资源具有了某些属性，用户（包括超级用户）都不能进行超出这些属性规定的访问，即不论用户的访问权限如何，只按照资源自身的属性实施访问控制。如某文件具有只读属性，对其有读写权限的用户也不能对该文件进行写操作。要修改目录或文件的属性，必须有对该目录或文件的修改权；要改变用户对目录或文件的权限，用户必须具有对该目录或文件的访问控制权。属性可以控制访问权限不能控制的权限，如可以控制一个文件是否可以同时被多个用户使

用等。

④ 身份验证

身份验证是证明某人是否为合法用户的过程,它是信息安全体系中的重要组成部分。

身份验证的方法有很多种,不同方法适合于不同的环境,网络组织可以根据自己的情况加以选择。以下是几种常用的身份验证方法。

- 用户名和口令验证。这是一种最简单的身份验证方法,也是大家用得最多、最熟悉的方法,在前面已经有所介绍。
- 数字证书验证。数字证书是 CA 认证中心签发的用于对用户进行身份验证的一种"执照"。数字证书的内容在 4.4.2 节中介绍。
- Security ID 验证。Security ID 已成为令牌身份验证事实上的标准,许多应用软件都能配置成支持 Security ID 作为身份验证手段的模式。Security ID 需要有一个能够验证用户身份的硬件装置(安全卡),该卡上有一个显示一串数字的液晶屏幕,其数字每分钟变化一次。用户在登录时先输入自己的用户名,然后输入卡上显示的数字。系统通过对用户输入的数字进行验证,如果数字正确,用户则通过了身份验证,即可进入系统了。
- 用户的生理特征验证。该验证是通过对用户人体的一处或多处生理特征检测而进行的验证。众所周知,每个人的指纹是不一样的,因此指纹是最常见的人体特征,可用来进行身份验证。此外,人们的视网膜、面部轮廓、笔迹、声音等都可作为人体特征用来进行身份验证。
- 智能卡验证。智能卡的外观和手感就像一张信用卡,但其原理就像一台小型计算机。智能卡是可编程的,卡里有一个处理器,具有存储和处理能力,可用来对数值进行运算,可无数次地接收写入信息,可下载应用软件和数据,然后可多次反复地使用它。用户在登录计算机网络时,可用它来证明自己的身份。不仅如此,它还可以代替身份证、旅行证件、信用卡、出入证等多种现代生活中离不开的证件。

⑤ 网络端口和节点的安全控制

网络中服务器的端口往往使用自动回呼设备、静默调制解调器加以保护,并以加密的形式来识别节点的身份。自动回呼设备用于防止假冒合法用户,静默调制解调器用以防范黑客的自动拨号程序对计算机进行的攻击。网络还常对服务器端和用户端采取控制,用户必须携带证实身份的验证器(如智能卡、磁卡、安全密码发生器等),在对用户的身份进行验证合法之后,才允许用户进入用户端。然后,用户端和服务器端再进行相互验证。

3.2.2 网络操作系统漏洞与补丁程序

1. Windows 系统的安全漏洞

虽然 Windows NT 系统采用了较强的安全性规则,但该系统还是存在许多安全漏洞。而 Windows 2000 系统面世不久,就被发现存在安全漏洞。如果用户不能对这些漏洞进行及时的补救,系统就可能被攻击,造成不必要的损失。

Windows NT/2000 系统有如下常见的漏洞。

- SAM 数据库漏洞。

- SMB 协议漏洞。
- Registry 数据库权限漏洞。
- 权限设置漏洞。
- 建立域别名漏洞。
- 登录验证机制漏洞。
- NetBIOS 漏洞。
- Telnet 漏洞。
- 奇怪的系统崩溃漏洞。
- IIS 服务泄露文件内容。
- ICMP 漏洞。

2. 补丁程序

补丁程序是指对于大型软件系统(如微软操作系统)在使用过程中暴露的问题(一般由黑客或病毒设计者发现)而发布的解决问题的小程序,就像发现衣服有破洞了就要打补丁一样,软件的补丁用来修补软件程序的“漏洞”。因为软件是人写的,编程人员在编程时也有考虑不周、不完善的地方,软件会出现 BUG,而补丁是专门修复这些 BUG 的。原来发布的软件存在缺陷,发现之后另外编制一个小程序对其缺陷进行弥补,使其完善,这种小程序就称为“补丁”。补丁是由软件的原作者制作的。

补丁程序主要有系统补丁和软件补丁。系统补丁顾名思义就是操作系统的不定期错误漏洞修复程序,如微软、UNIX、Linux 等操作系统的补丁。软件补丁通常是因为发现了软件的小错误,为了修复个别小错误而推出的,或者为了增强某些小功能而发布的,或者是为了增强文件抵抗计算机病毒感染而发布的补丁,如微软的 Office 为了抵抗宏病毒而打补丁。

3. 补丁程序的安装

常用的“打补丁”的方法有两种,即利用软件的自动更新(Update)功能和手工操作。

(1) 利用系统的 Update 功能打补丁

如果软件提供了 Update(自动更新)功能,打补丁就是一件非常简单的事情,只需要在“开始”菜单中找到 Update 命令,单击后即可自动上网搜索官方网站,检查有无最新版本或者补丁程序。

(2) 手工打补丁

多数补丁需要先在开发商网站或软件下载网站下载,然后再在本机上运行相应命令来完成。有些补丁需要按照一定操作步骤来完成,因此在打补丁之前要先仔细阅读其说明文档,以免产生错误,造成不可挽回的损失。

一些重要软件产品的补丁网址和主要公司的补丁网站如下:

Windows 2000 安全补丁(Windows 2000 Service Pack 2)的下载网址是 http://www8.pconline.com.cn/download/swdetail.phtml?id=1746。

Windows 2000 安全补丁集(Windows 2000 Security RollupPackage)的下载网址是 http://202.102.231.142/code/fixdown/down/download.asp?id=2209&tp=filename。

微软公司的补丁网站是 http://www.microsoft.com/china/msdownload/?MSCOMTB=

MS_Products|,Macromedia 公司的补丁网站地址是 http://www.macromediachina.com/downloads,专门的补丁网站地址是 http://www.mypatch.net。

3.3 网络操作系统的安全设置实践

3.3.1 Windows 系统的安全设置

目前使用 Windows 操作系统的用户非常多,但 Windows 并不是一款安全的操作系统。计算机病毒、黑客时时威胁着 Windows 系统,因此 Windows 系统的安全问题越来越受到人们关注。虽然 Windows 的漏洞众多,安全隐患也很多,但经过适当的设置和调整,还是可以使 Windows 系统达到相对安全的。下面介绍 Windows 系统常见的安全设置方法,其中大部分操作都是针对 Windows 2000/2003/XP 的。

1. 用户安全设置

(1) 管理员账号管理

① 创建两个管理员账号

系统可创建两个管理员账号,一个是具有一般权限的普通账号,一个是具有最高权限的 Administrator。平时利用具有一般权限的普通账号接收信息和处理一些日常事务,而 Administrator 只在特殊需要或关键时刻使用。

② 把 Administrator 账号改名并创建一个陷阱账号

众人皆知 Administrator 是管理员账号,为了不使其成为众矢之的,有效地防止别人对它尝试攻击或破译,可将 Administrator 改为一个普通的名字(不要使用 Admin)。将 Administrator 改名后,再创建一个名为 Administrator 的本地账号,把它的权限设置成最低,并为其设置一个超级复杂密码。这样可以使那些别有企图的人找不到真正的管理员,借此还有可能发现它们的入侵企图。

③ 使用安全密码

为账号选择一个安全密码是非常重要的,但这却是最容易被忽略的。一些部门的管理员创建账号时,往往用公司名、计算机名等做用户名,然后又把这些账号的密码设置得很简单,如"welcome"、"iloveyou"或与用户名相同。用户在首次登录时就应该为这些账号设置复杂的密码,并注意经常更换这些密码。

(2) 一般用户账号管理

① 禁用或激活用户账号

- 使用计算机管理员身份登录(若使用受限用户登录系统,后续工作就不能完成;如果计算机与网络连接,则网络策略设置也可以阻止用户完成后续操作)。
- 登录系统后,选择菜单"开始"→"程序"→"管理工具"→"计算机管理",打开"计算机管理"窗口。依次展开窗口左侧列表中的"计算机管理(本地)"→"系统工具"→"本地用户和组"→"用户",这时在窗口右侧显示了系统中所有的用户账号,如图 3.1 所示。



图 3.1　显示系统中所有的用户账号

- 如果管理员想禁用哪个用户账号，可以选中该用户账号，然后单击鼠标右键，在弹出的菜单中选择“属性”，打开该账号的“属性”窗口。在该窗口的“常规”标签中选择“账号已停用”复选框，如图 3.2 所示。然后单击“确定”按钮，这样此账号就被禁用了。如果想激活被禁用的账号，可以将“账号已停用”复选框的选择取消，即可激活该用户。



图 3.2　账号属性

② 为账号双重加密

用户可使用系统的组策略工具对用户账号密码设置进行限制，这样可保护自己的账号安全。

- 在“开始”→“运行”对话框中输入 syskey，按回车键后可打开“保证 Windows XP 账号数据库的安全”对话框，如图 3.3 所示。该项操作是不可逆的，一旦启用加密则不可以禁用。在这里若直接选中“启用加密”选项，并单击“确定”按钮，程序就对账号完

成了双重加密，只不过该加密过程对用户来说是透明的。

- 如果用户想进一步体验这种双重加密功能，则可在"保证 Windows XP 账号数据库的安全"对话框中单击"更新"按钮，打开"启动密码"对话框，如图 3.4 所示。在这里有"密码启动"和"系统产生的密码"两个选项。

若选择"密码启动"则需要自己设置一个密码，这样在登录 Windows XP 之前要先输入该密码然后才能选择登录的账号。

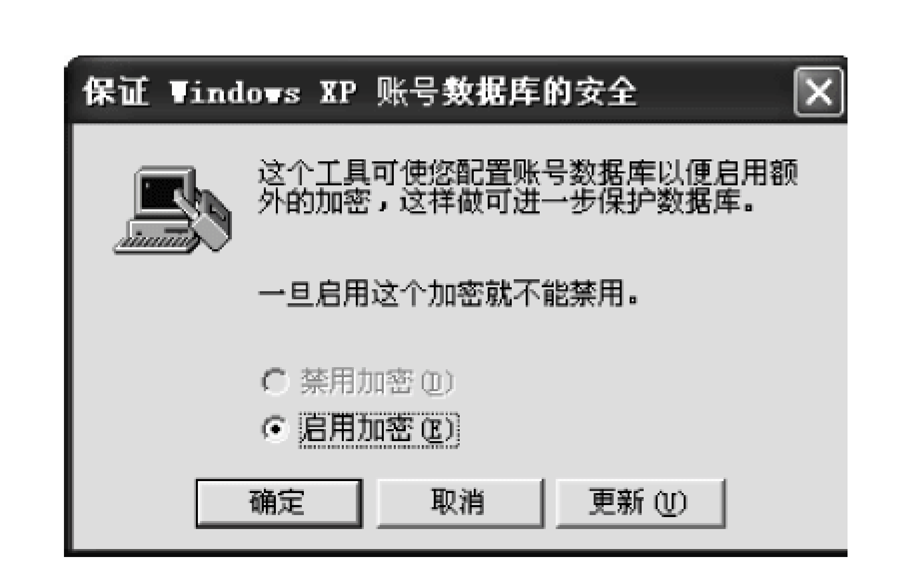


图 3.3 为账号双重加密

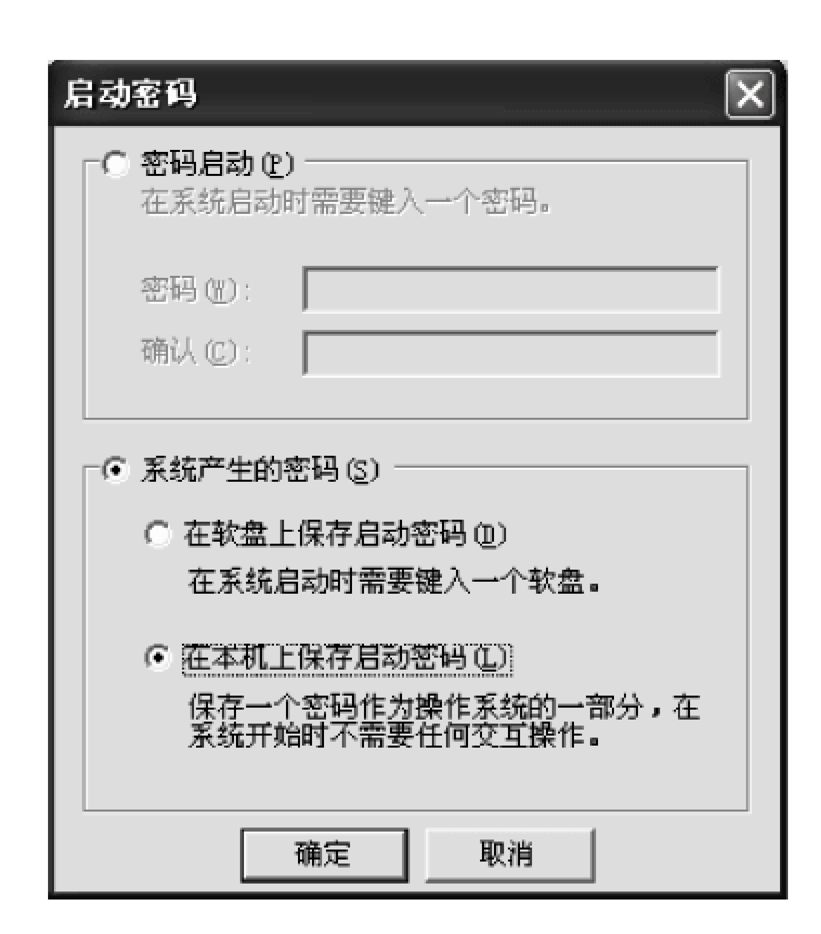


图 3.4 "启动密码"对话框

在"系统产生的密码"选项下又有两个选项。若选择"在本机上保存启动密码"选项，则程序仅在后台完成加密过程。在登录时不需要输入任何密码，因为密码就保存在计算机内部。如果用户对安全保密要求比较高，则可以选择"在软盘上保存启动密码"选项，单击"确定"按钮后，就会有提示在软驱里放入一张软盘。创建完毕，会在软盘上生成一个 StartKey.key 文件，以后每次开机时则必须放入该软盘才能登录，相当于系统有了一张可以随身携带的钥匙盘。

③ 重命名和禁用默认的账号

安装好 Windows 后，系统会自动建立两个账号：Administrator 和 Guest，其中 Administrator 是管理员账号，它拥有最高的权限；Guest 是来宾账号，它只有基本的权限且默认是禁用的。而这种默认账号在为用户带来方便的同时也严重危害到了系统安全。因此，安全的做法是把 Administrator 账号的名称改掉，然后再建立一个几乎没有任何权限的假 Administrator 账号，以迷惑入侵者。具体操作如下：

- 选择菜单"开始"→"运行"，输入 secpol.msc 后按回车键，打开"本地安全设置"对话框。
- 依次展开"本地策略" →"安全选项"，在右侧窗口有一个"账号：重命名系统管理员账号"的策略。
- 双击打开后可以给 Administrator 重新设置一个不是很引人注目的用户名(如 ABCD)，如图 3.5 所示。

然后还可以再新建一个名称为 Administrator 的受限制用户，以假乱真。



图 3.5　Administrator 重命名设置

④ 删除不必要的用户账号

Guest 账号很容易被入侵者用来攻击系统，因此，为了安全起见，可以考虑将该账号停掉，任何时候都不允许 Guest 账号登录系统。

管理员可利用用户组策略设置相应权限，并经常检查系统账号，删除已经不用的账号。因为这些无用账号很多时候都是黑客入侵系统的突破口，系统的账号越多，黑客得到合法用户的权限可能性一般也就越大。为了安全起见，限制系统中的用户数量是必要的，因此可以将系统中的 duplicateuser 账号、测试用账号、共享账号等删除。

(3) 用户登录和密码安全

① Administrator 账号登录

在 Windows XP 下，如果建立了一个新的非受限制用户(计算机管理员，如 QAZ)，下次登录计算机时，将不会出现 Administrator 超级用户的登录入口了。当必须使用 Administrator 账号登录时，可以采用以下方法：

以现有的计算机管理员 QAZ 账号登录，选择菜单“程序”→“管理工具”→“计算机管理”→“系统工具”→“本地用户和组”，然后单击“用户”，即可看到 Administrator 账号，如图 3.6 所示。



图 3.6　本地计算机用户

将当前的计算机管理员账号 QAZ 停用或删除后，就可以用 Administrator 用户登录了。其操作为：右击 QAZ，选择“属性”选项，勾选“账号已停用”复选框后，单击“确定”按钮，这样就停用了该账号。停用后的该账号前有个红色的叉号显示，如图 3.6 所示。这样重新启动计算机时就会出现 Administrator 账号的登录入口了。

② 找回 Administrator 账号密码

Windows XP 安装在 NTFS 分区上。在使用故障修复控制台时，程序要求输入 Administrator 的密码，但此时却忘记了密码(安装 Windows XP 时设置了密码)。可用以下方法找回 Administrator 的密码。

- 若能正常进入 Windows XP，则使用具有管理员权限的账号登录 Windows XP，然后打开如图 3.6 所示的计算机本地用户栏，可以看到当前系统里存在的全部账号。右击 Administrator，选择“设置密码”，然后按照屏幕提示操作即可重新设置密码，如图 3.7 所示。

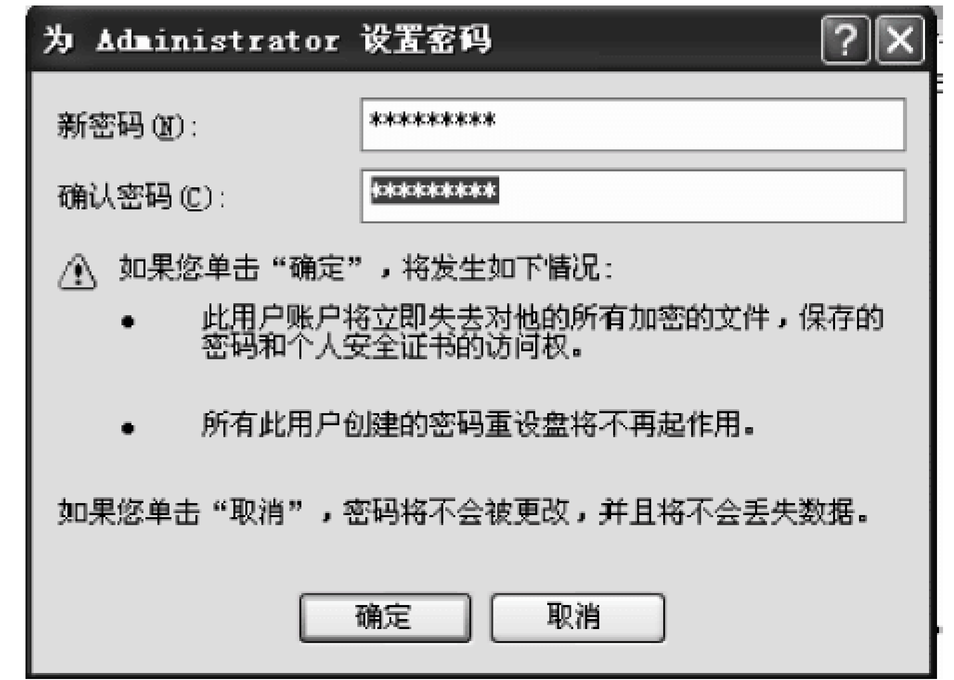


图 3.7　重新设置密码

- 若无法正常进入 Windows XP，如果可以使用命令行安全模式，则可用具有管理权限的账号登录，使用 NETUSER 命令修改密码，格式为“NETUSERAdministrator(输入你的新密码)”，然后按回车键即可。
- 如果连命令行安全模式都无法进入，那么只有使用安装光盘选择修复了。用安装光盘启动系统时，在安装程序选择菜单上选择“现在运行安装 Windows”，然后选择“修复”开始修复程序。修复过程类似于 Windows 98 的覆盖安装，修复中会要求重新创建密码，而且已经安装的软件仍然可以继续使用。

③ 找回丢失的系统密码

当管理员密码丢失或被改动，可采用以下方法恢复。

第 1 种方法　从 SAM 文件中破解密码。

SAM 文件是 Windows XP 的用户账号数据库，所有 Windows XP 用户的登录名及口令等相关信息都保存在该文件中。SAM 文件位于“C:\system32\config\sam”路径下，如果删除了 SAM 文件，在登录 XP 时就不需要密码了，但是账号中包含的一些信息(如所创建的用户及用户组)也随之丢失。

第 1 步：将丢失账号的硬盘接到正常系统中，然后运行 LC4(一款暴力破解软件)，在程序界面的菜单上选择菜单 Flie→NewSession 来新建一个任务，接着选择菜单 Import→ImportfromSAMfile。

第 2 步：在弹出的对话框中找到并打开待破解的 SAM 文件，此时 LC4 会自动分析此文件，并显示文件中的用户名，确认这个账号是欲破解的目标后，单击 Session→BeginAudit 菜单命令即可开始破解密码。如果密码不是很复杂，很快就能得到结果；如果密码比较复杂，需要的时间会较长。

第 2 种方法　利用密码重设盘恢复密码。

第 1 步：打开“控制面板”窗口，选择“用户账号”，单击欲备份密码的账号，在弹出的账号操作窗口中“相关任务”栏下方，单击“阻止一个已忘记的密码”选项，如图 3.8 所示。

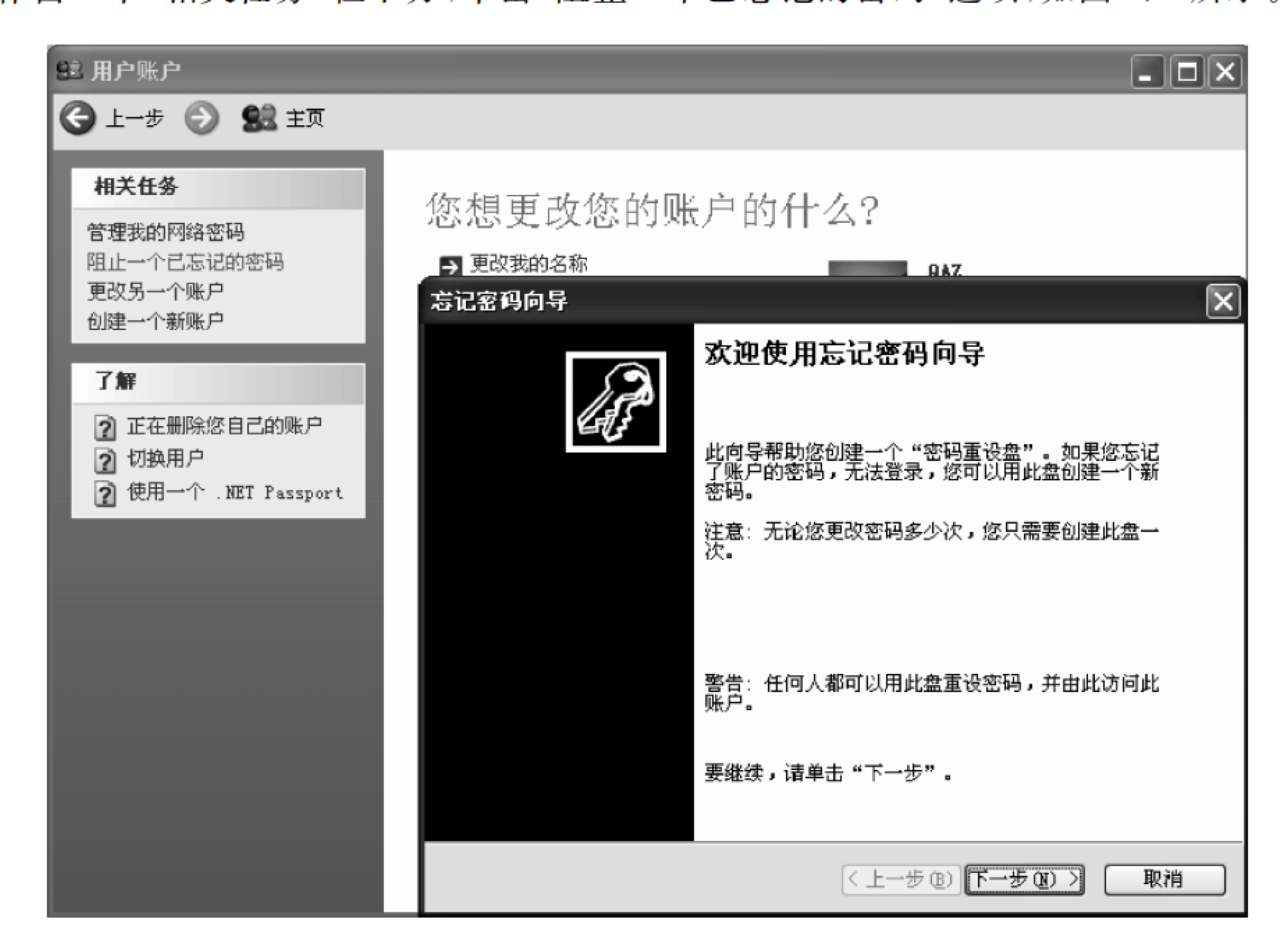


图 3.8　进入“忘记密码向导”

第 2 步：打开“忘记密码向导”对话框，单击“下一步”按钮，根据提示在软驱中插入一张空白已格式化的软盘，单击“下一步”按钮，输入当前账号的密码，再次单击“下一步”按钮，即可完成密码重设磁盘的创建，如图 3.9 所示。



图 3.9　输入当前账号密码

第3步：当忘记密码需要使用密码重设盘时，可先启动 Windows XP，在出现录入窗口时，单击用户名，然后随意输入密码。由于输入密码错误，所以系统会给出“没有记住密码?”的提示，这时利用生成的密码重设盘，根据提示即可进行密码的恢复工作了。

2. 系统安全设置

(1) 使用文件加密系统 EFS

Windows 系统强大的文件加密功能可给磁盘、文件夹和文件加上一层安全保护。这样可以防止别人把用户的硬盘挂到别的机器上以读出里面的数据。有关 EFS 的内容可见5.2节。

(2) 目录和文件权限设置

① 访问权限设置

先创建一个用户组，以后所有站点的用户都建在这个组里；再设置该组在各个分区没有权限或者完全拒绝；然后设置各用户在各自文件夹里的权限。

- 对 Windows 用户，在系统中可按用户(组)来划分权限。选择菜单“开始”→“程序”→“管理工具”→“计算机管理(本地)”→“本地用户和组”，在这里可详细管理系统用户和用户组。
- NTFS 权限设置。分区时可把所有的硬盘都分为 NTFS 分区，然后确定每个分区对每个用户开放的权限。右击要设定权限的文件或文件夹，选择“属性”→“安全”标签，在这里可管理 NTFS 文件(夹)权限。

② 设置文件共享权限

在局域网中，经常要进行访问或互相交换文件。但是在 Windows XP 系统的常规共享设置中只可以设置成只读共享和完全共享，没有共享权限设置，这直接影响到共享文件的安全性。而在 Windows 2000 的共享设置中也不能像 Windows 98 一样直接设置访问密码。其实在 Windows 2000/XP 中是能设置共享密码的，只不过操作方法不同而已。

- 简单文件共享

打开“我的电脑”窗口，依次选择菜单“工具”→“文件夹选项”，打开“文件夹选项”对话框，选择“查看”选项卡，在“高级设置”列表中选择“使用简单文件共享(推荐)”复选框，如图3.10所示。

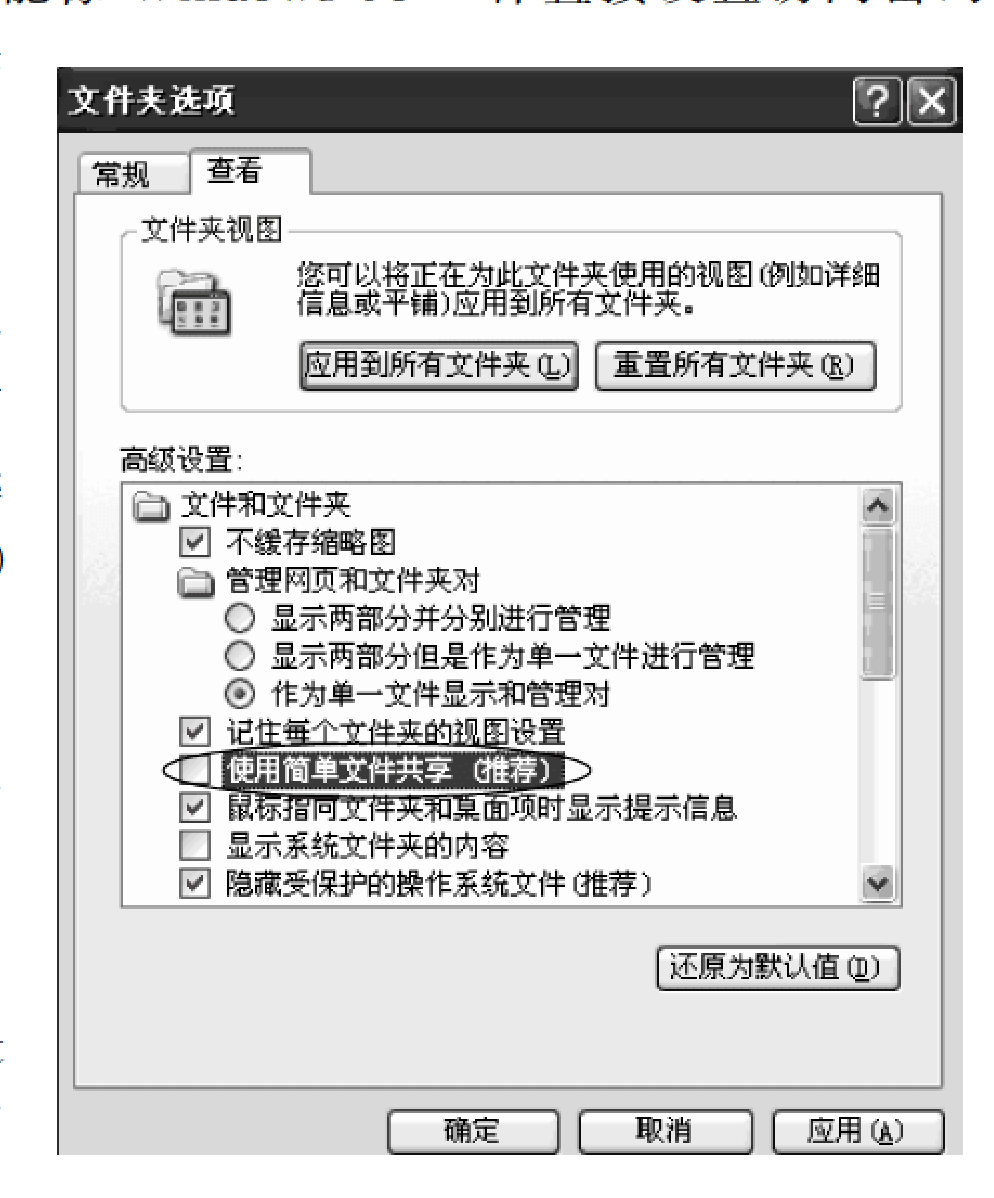


图3.10 简单文件共享

- 启动 Guest 账号

在系统的默认状况下，Guest 账号是没有启用的。如要想让局域网中的其他用户能访问你的计算机，首先就得启用该账号。选择“控制面板”→“用户账号”菜单，单击界面中的“Guest 账号”，然后再单击“启用来宾账号”按钮，即可完成 Guest 账号的启动，如图3.11所示。



图 3.11　启动 Guest 账号

• 添加共享访问用户

由于用户在访问共享资源时,需要根据不同的用户设置不同的访问权限,所以在这里所添加的共享访问用户也要设置多个权限的用户和密码,以供用户访问。

第 1 步:打开"控制面板"中的"用户账号",单击"创建一个新账号",这时会提示为新账号键入一个名称,输入一个要创建的用户名(如 ABCD),单击"下一步"按钮,然后系统会提示选择账号类型,有计算机管理员和受限用户两个账号类型供选择。鉴于安全考虑,选择创建受限用户,如图 3.12 所示。

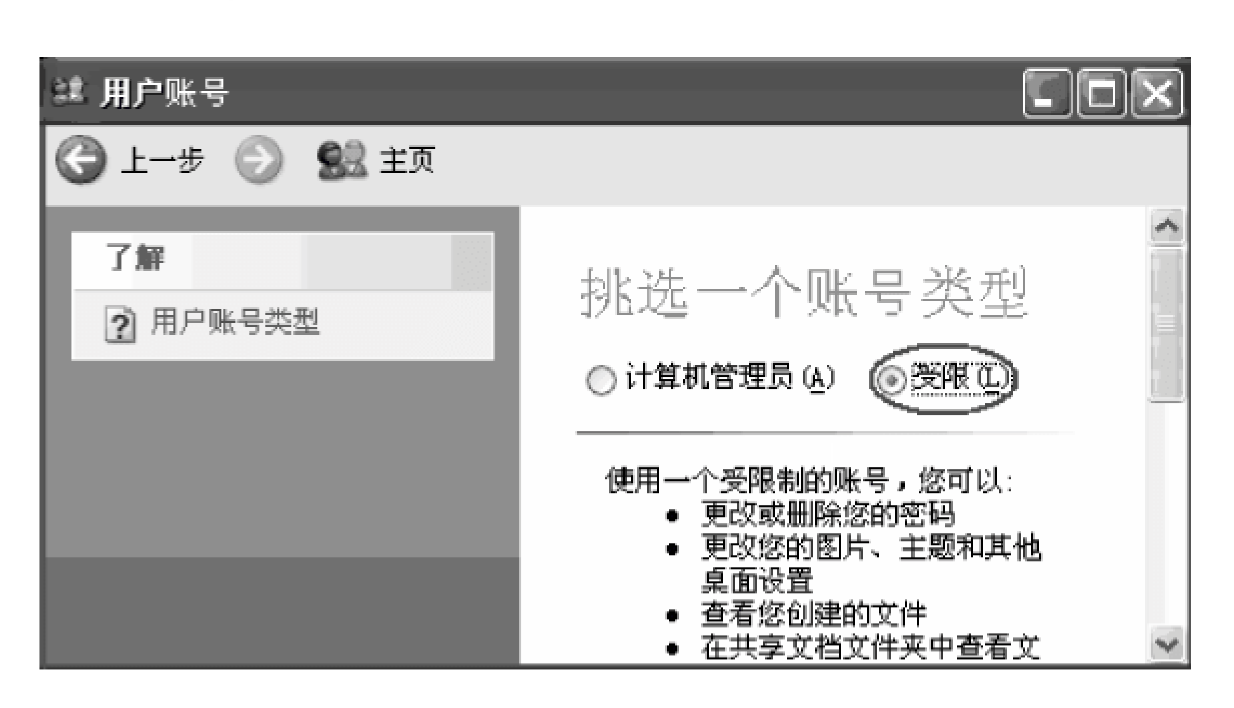


图 3.12　创建受限账号

第 2 步:完成以上操作后,在"用户账号"的主界面中就多了一个"ABCD"受限账号,如图 3.13 所示。然后再为该用户设置访问密码。在"用户账号"主界面中单击"ABCD"账号,再单击"创建密码",进入创建密码对话框。在为 ABCD 用户创建密码对话框中输入并验证新创建账号的密码,并设置一个密码提示语,最后单击"创建密码"按钮即可,如图 3.14 所示。

• 设置共享资源

在完成以上操作后,就可以设置共享了。

第 1 步:选择一个要共享的文件或文件夹并右击,选择"共享和安全",这时的界面已与先前共享的界面不同了,多了"权限"和"缓存"设置项。

第 2 步:选择"共享该文件夹",单击"权限"按钮,在"权限"设置窗口中先删除已有的



图 3.13　完成创建受限账号 ABCD

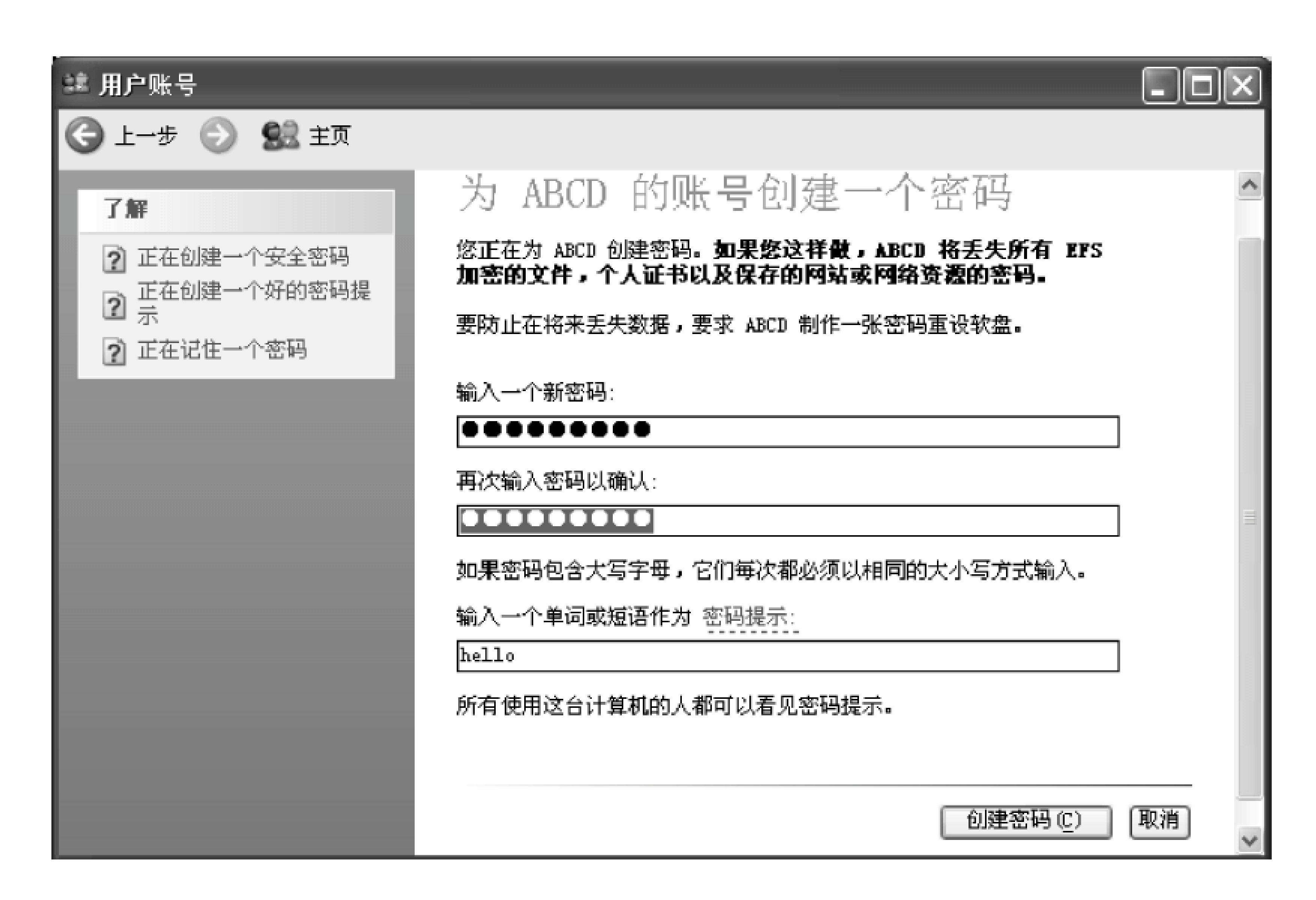


图 3.14　为 ABCD 账号设置密码

"Everyone"，接着添加刚才所创建的用户。依次单击"添加"→"高级"→"立即查找"菜单命令，搜索系统中已有的用户和组。最后在界面下方的用户和组的列表中选择"ABCD"账号，单击两次"确定"按钮回到权限设置窗口。

③ 设定安全记录的访问权限

在默认情况下安全记录是没有保护的，可把它设置成只有 Administrator 和系统账号才有权访问。

(3) 备份系统和数据

用 ghost 软件及时对 C 盘做好备份，并用 KV2008、PQ 等软件将硬盘的分区表进行备

份。同时，还需要制作一张启动盘以便必要时使用。

使用 ntbackup 软件备份系统状态，使用 reg. exe 备份系统关键数据，如 reg export HKLM\SOFTWARE\ODBC e:\backup\system\odbc. reg/y，即可将 SOFTWARE 下的 ODBC 文件备份到 E 盘。

(4) 安装系统补丁程序

安装系统补丁的重要性是不言而喻的，尤其是一些重要的安全补丁和针对 IE、OE 漏洞的补丁。尽量安装最新的操作系统和浏览器，并通过下载安装补丁对系统进行升级。Microsoft 会经常发布一些已知漏洞的修补程序，这些程序一般都可以通过 Windows Update 来安装(可经常性地访问 Windows Update 网站或者直接单击"开始"菜单中 Windows Update 的快捷方式)。而 Windows XP 和最新的 Windows 2000 更加先进了，可以自动检查更新，在后台下载，完成后通知下载完成并询问是否开始安装。对于 Windows 2000/XP 的用户，Microsoft 还提供了一个检查安全性的实用工具——基准安全分析器(Microsoft Baseline Security Analyzer)。该程序可以自动对用户的系统进行安全性检测，并且对于出现的问题，都可以提供一个完整的解决方案，它非常适合对于安全性要求高的用户使用。

(5) 禁止管理共享

进入注册表，打开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 项。对于服务器，添加键值 AutoShareServer，类型为 REG_DWORD，其值为 0。对于客户机，添加键值 AutoShareWks，类型为 REG_DWORD，其值为 0。

(6) 设置屏幕保护密码

设置屏幕保护密码是很必要的，操作也很简单，这也是防止内部人员破坏服务器的一个屏障。屏幕保护密码不需要很复杂，因为没必要浪费很多系统资源。系统用户所使用的机器最好也加上屏幕保护密码。

(7) 防范 SYN 攻击

系统可使用 SYN 淹没攻击保护，进入注册表，打开 HKLM\SYSTEM\CurrentControlSet\Service\Tcpip\Parameters，相关的值项如下：

- DWORD：SynAttackProtect　定义了是否允许 SYN 淹没攻击保护，值为"1"表示允许启用 Windows 2000 的 SYN 淹没攻击保护。
- DWORD：TcpMaxConnectResponseRetransmissions　定义了对于连接请求回应包的重发次数。值为"1"，则 SYN 淹没攻击不会有效果，但是这样会使连接请求失败的概率增大。SYN 淹没攻击保护只有在该值≥2 时才会被启用，默认值为 3。
- DWORD：TcpMaxHalfOpen　定义了能够处于 SYN_RECEIVED 状态的 TCP 连接数目，默认值为 100。
- TcpMaxHalfOpenRetried　定义了在重新发送连接请求后，仍处于 SYN_RECEIVED 状态的 TCP 连接数目，默认值为 80。
- TcpMaxPortsExhausted　定义了系统拒绝连接请求的次数，默认值为 5。

上述前两项定义了是否允许 SYN 淹没攻击保护，后三项定义了激活 SYN 淹没攻击保护的条件，满足其中之一，则系统自动激活 SYN 淹没攻击保护。

(8) 预防 DoS

进入注册表,打开 HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters,更改以下值可以防御一定强度的 DoS 攻击:

```
SynAttackProtectREG_DWORD 2
EnablePMTUDiscoveryREG_DWORD0
NoNameReleaseOnDemandREG_DWORD 1
EnableDeadGWDetectREG_DWORD 0
KeepAliveTimeREG_DWORD300,000
PerformRouterDiscoveryREG_DWORD 0
EnableICMPRedirectsREG_DWORD 0
```

(9) 加密 temp 文件夹

一些应用程序在安装和升级的时候,会把一些内容复制到 temp 文件夹下,但是当程序升级完毕或关闭时,并不会自动清除 temp 文件夹中的内容。所以,给 temp 文件夹加密也可使文件多一层保护。

(10) 清空远程可访问的注册表路径

Windows 2003 系统提供了注册表的远程访问功能。当将远程可访问的注册表路径设置为空时,才能有效地防止黑客利用扫描器通过远程注册表读取计算机的系统信息。设置远程可访问的注册表路径为空的步骤如下:

① 选择“开始”→“运行”菜单命令,输入 gpedit.msc,确认后打开组策略编辑器。

② 在组策略中,展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”。

③ 单击“安全选项”,在右侧窗口中找到“网络访问:可远程访问的注册表路径”,并双击之,如图 3.15 所示。



图 3.15 进入远程可访问的注册表路径

④ 在打开的“网络访问:可远程访问的注册表路径 属性”窗口中,将可远程访问的注册表路径和子路径内容全部设置为空,再单击“确定”按钮即可。

另外,在进行安全设置中,对如图 3.15 所示的本地策略的安全选项设置可以考虑将“网

络访问：可匿名访问的共享”、“网络访问：可匿名访问的命名管道”和“网络访问：可远程访问的注册表路径”三项全部删除；将“网络访问：不允许 SAM 账号的匿名枚举”、“网络访问：不允许 SAM 账号和共享的匿名枚举”、“网络访问：不允许为网络身份验证储存凭据或 .NET Passports”和“网络访问：限制匿名访问命名管道和共享”四项更改为“已启用”。

（11）利用“密码策略”设置可靠的密码

尽管绝对安全的密码是不存在的，但是相对安全的密码还是可以实现的。这还需要运行 secpol.msc 来配置“本地安全设置”。展开“账户策略”→“密码策略”，如图 3.16 和图 3.17 所示。经过对这里策略的配置，就可以建立一个完备密码策略，使密码可以得到最大限度的保护。账号密码配置如下：



图 3.16　安全选项的设置



图 3.17　账号的密码配置

① 强制密码历史

该设置决定了保存用户曾经用过的密码个数。很多人知道要经常性的更换自己的密码，可是换来换去就是有限的几个在轮换。配置该策略就可以知道用户更换的密码是否是以前曾经使用过的。默认情况下，该策略不保存用户的密码，用户可以自己设置，建议保存 5 个以上(最多可以保存 24 个)。

② 密码最长存留期

该策略决定了一个密码可以使用多久，之后就会过期，并要求用户更换密码。如果设置

为 0,则密码永不过期。一般情况下设置为 30～60 天就可以了,最长可以设置 999 天。具体的过期时间要看系统对安全要求的严格程度。

③ 密码最短存留期

该策略决定了一个密码要在使用多久之后才能再次被使用。如果设置为 0,则表示一个密码可以被无限制地重复使用。

④ 密码长度最小值

该策略决定了一个密码的长度,有效值在 0～14 之间。如果设置为 0,则表示不需要密码;该数字越大,表示密码的位数越多,密码安全程度越高。建议的密码长度≥6 位。

⑤ 密码必须符合复杂性要求

如果启用了该策略,则在设置和更改密码时,系统将会按照一定的规则检查密码是否有效。

⑥ 为域中所有用户使用可还原的加密来储存密码。很明显,该策略最好不要启用。

(12) 删除默认共享

使用 Windows 2003 的用户都会碰到一个问题,就是系统在默认安装时都会产生默认的共享文件夹。虽然用户并没有设置共享,但每个盘符都被 Windows 自动设置了共享,其共享名为盘符后面加一个符号 $(共享名分别为 c$、d$、ipc$ 等)。这样,只要攻击者知道了该系统的管理员密码,就有可能通过输入"\\工作站名\共享名称"来打开系统的指定文件夹,用户精心设置的安全防范就不安全了。因此,应将 Windows 2003 系统默认的共享隐患从系统中清除掉,可采用以下步骤:

① 选择"开始"→"运行"菜单,输入 gpedit.msc,确认后打开组策略编辑器。

② 选择"用户配置"→"Windows 设置"→"脚本(登录/注销)"菜单,双击"登录"脚本,在出现的"登录属性"窗口中单击"添加"按钮,如图 3.18 所示。



图 3.18 利用组策略删除默认共享

③ 在出现的"添加脚本"对话框中的"脚本名"栏中输入 delshare.bat，然后单击"确定"按钮即可。

重新启动计算机系统后，就可以自动将系统所有的隐藏共享文件夹全部取消。

(13) 卸载不安全组件

当在系统中加入不安全组件检测功能后，就可发现使用的服务器支持的很多组件是不安全的。但这些不安全也是相对的，只要做好相关的设置，原来不安全的组件就会安全了。

如果有些组件是不安全的，且对用户来说又可能没有什么用途，在系统安装后就可以将它们删除掉(卸载)。决定是否卸载一个组件时一定要谨慎。因为组件是为了应用而出现的，所有的组件都有它的用处，所以在卸载一个组件前，必须明确该组件确实是系统不需要的。比如，FSO 和 XML 都是常用的组件，很多程序会用到它们。WSH 组件会被一部分主机管理程序用到，有的打包程序也会用到它。

最危险的组件是 WSH 和 Shell，因为它们可以运行硬盘里的.exe 程序，比如可以运行提升程序来提升 SERV-U 权限，甚至用 SERV-U 来运行更高权限的系统程序。因此，用户可以卸载 WSH 和 Shell 这两个组件。卸载组件的最简单办法就是直接卸载后删除相应的程序文件。

例 3-1　卸载 WSH 和 Shell 组件。

将下面的代码保存为一个.BAT 文件：

```
regsvr32/u C:\WINDOWS\System32\wshom.ocx
delC:\WINDOWS\System32\wshom.ocx
  (利用 regsvr32 /u wshom.ocx 卸载 WScript.Shell 组件)
regsvr32/u C:\WINDOWS\system32\shell32.dll
delC:\WINDOWS\system32\shell32.dll
  (利用 regsvr32 /u shell32.dll 卸载 Shell.application 组件)
```

运行该批处理文件后，WScript.Shell 和 Shell.Application 组件就会被卸载。在卸载过程中，可能会出现无法删除文件的提示，可以不用管它，重启服务器即可。

例 3-2　卸载 FSO 组件。

使用 regsvr32/u c:windows\system32\scrrun.dll 卸载组件。在"开始"菜单下运行 regedit，打开注册表编辑器，将/HKEY_CLASSES_ROOT 下的 WScript.Network、WScript.Network.1、WScript.Shell、WScript.Shell.1、Shell.Application 和 Shell.Application.1 的键值改名或删除。在/HKEY_CLASSES_ROOT/CLSID 中包含的字串(如{72C24DD5-D70A-438B-8A42-98424B88AFB8})下找到相关的键值，如图 3.19 所示，并将其全部删除。

(14) 关闭不必要的端口

在系统安装后，为了安全起见，可关闭一些不需要的端口。具体步骤如下：

① 选择菜单"开始"→"设置"→"网络连接"→"本地连接"，打开"本地连接 属性"对话框，如图 3.20 所示。

② 选择"Internet 协议(TCP/IP)"选项，单击"属性"按钮，弹出"Internet 协议(TCP/IP)属性"对话框，如图 3.21 所示。

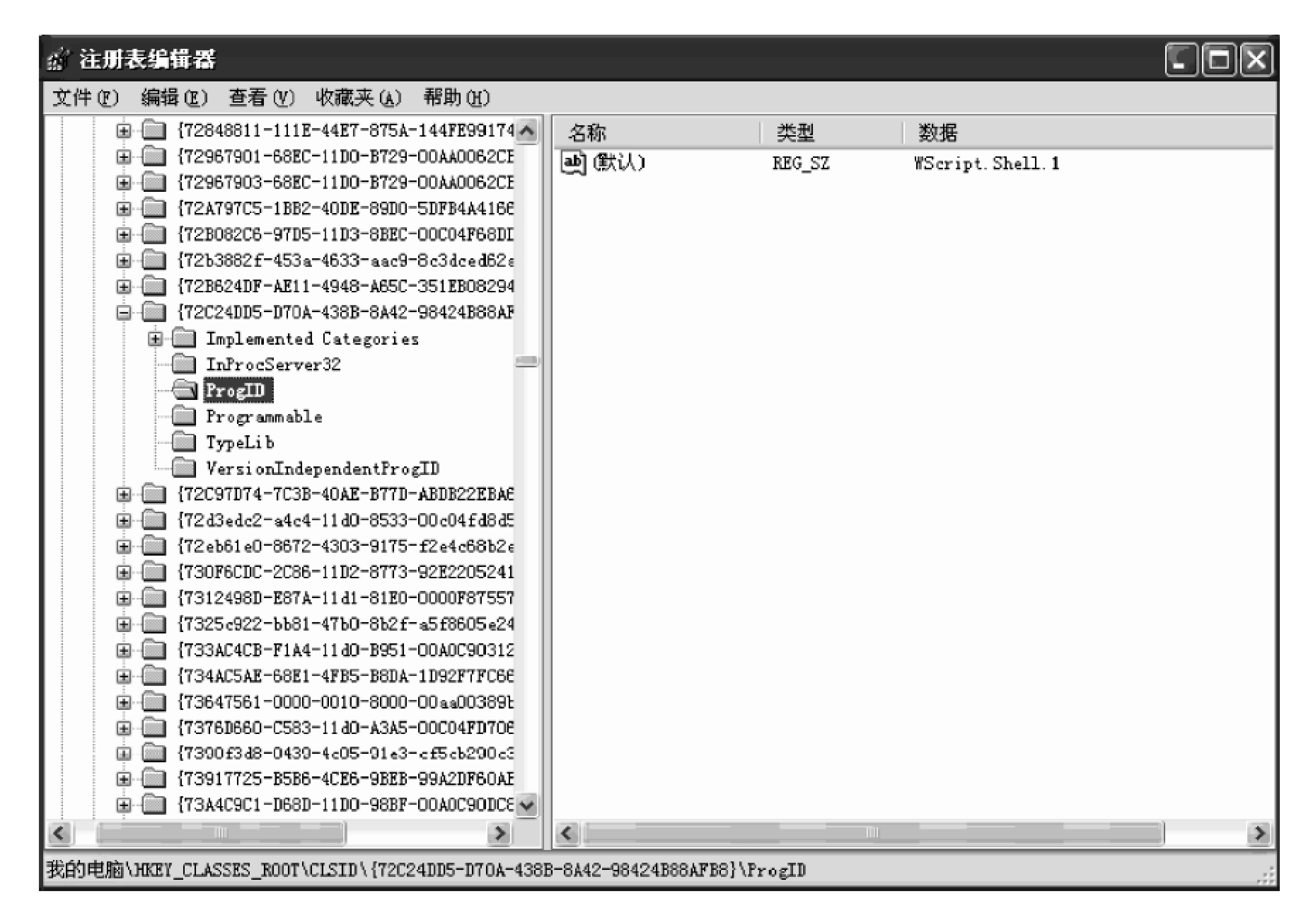


图 3.19 注册表修改或删除键值



图 3.20 “本地连接 属性”对话框

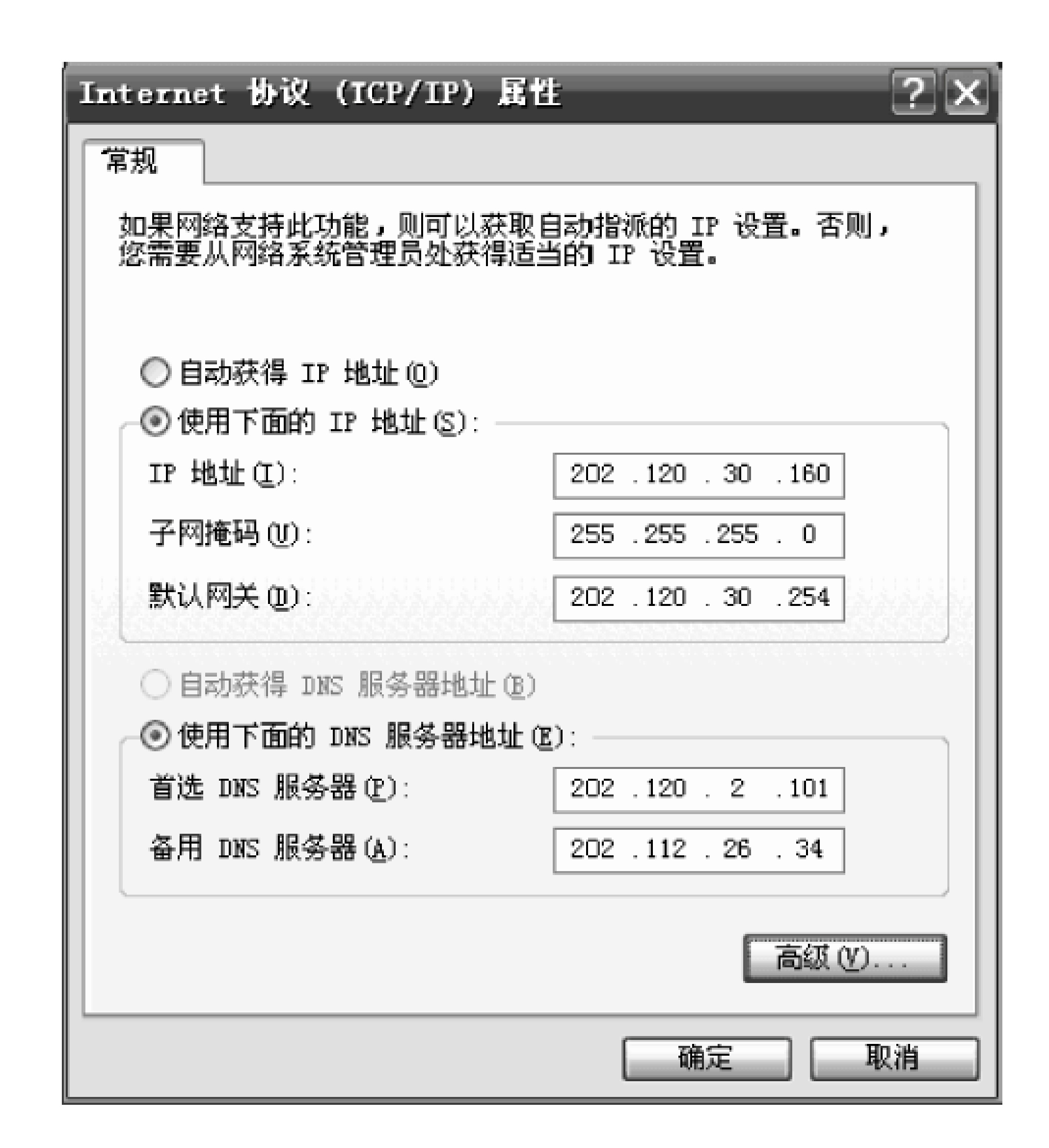


图 3.21 “Internet 协议(TCP/IP)属性”对话框

③ 单击“高级”按钮,弹出“高级 TCP/IP 设置”对话框,如图 3.22 所示。

④ 单击“选项”选项卡,弹出“TCP/IP 筛选”,单击“属性”按钮,打开 TCP/IP 筛选,添加需要的 TCP、UDP 协议即可,参见图 2.8。

(15) 杜绝非法访问应用程序

Windows 2003 是一种服务器操作系统。为了防止非法用户登录到系统中并随意启动

服务器中的应用程序，给服务器的正常运行带来不必要的麻烦。可根据不同用户的访问权限，来限制他们去调用应用程序。实际上只要使用组策略编辑器作进一步的设置，即可实现这一目的。具体步骤如下：

① 打开“组策略编辑器”，然后依次选择“本地计算机策略”→“用户配置”→“管理模板”→“系统”菜单。

② 选择“只运行许可的 Windows 应用程序”并双击，弹出如图 3.23 所示的窗口。



图 3.22　“高级 TCP/IP 设置”对话框



图 3.23　组策略编辑器的系统设置

③ 在图 3.24 中的“设置”标签中选择“已启用”，单击下面的“允许的应用程序列表”右边的“显示”按钮，弹出一个“显示内容”对话框。

④ 单击“添加”按钮来添加允许运行的应用程序，如图 3.24 所示。



图 3.24　允许的应用程序列表框

这样操作后一般用户只能运行“允许的应用程序列表”中的程序。

(16) 关闭自动播放服务

自动播放功能不仅对光驱起作用,而且对其他驱动器也起作用,这样很容易被黑客利用来执行黑客程序,因此,可以考虑关闭该服务。关闭自动播放服务的操作步骤如下:

① 打开组策略编辑器,依次展开“计算机配置”→“管理模板”→“系统”。

② 在右侧窗口中找到“关闭自动播放”选项,并双击。

③ 在打开的对话框中选择“已启用”选项,然后在“关闭自动播放”右面的下拉菜单中选择“所有驱动器”选项,单击“确定”按钮即可生效,如图 3.25 所示。

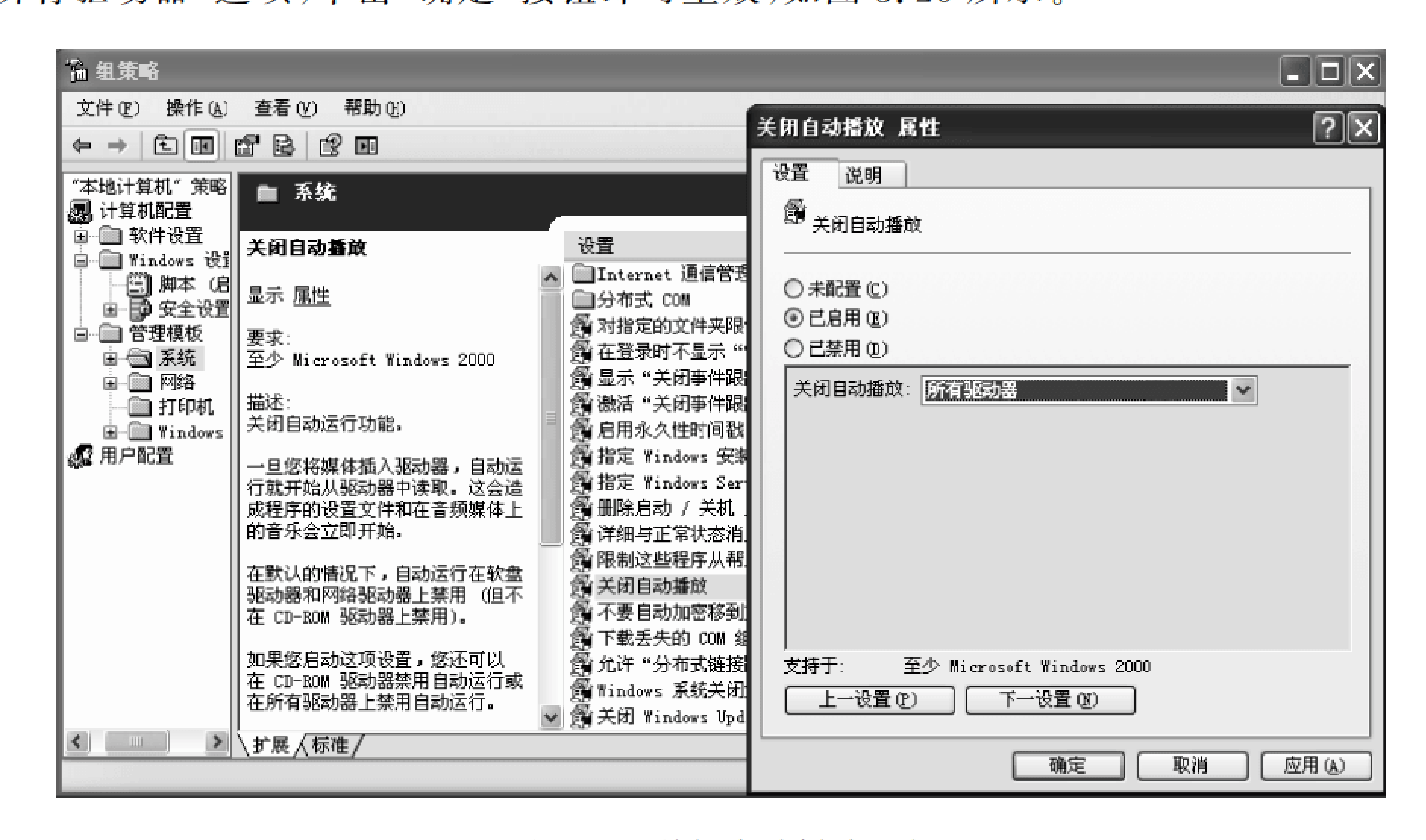


图 3.25 关闭自动播放服务

(17) 账户锁定设置

账户锁定策略是一项 Active Directory 安全功能。在指定时间段内,如果登录尝试失败次数达到指定次数,它会锁定用户账户并禁止登录。允许尝试的次数和时间段基于为账户锁定设置的值。账户锁定策略还可以指定锁定期限。账户锁定设置有助于防止攻击者猜测用户密码,并且会降低对网络环境攻击成功的可能性。账户锁定设置的过程为:

单击“开始”→“运行”命令,输入 secpol.msc,打开本地安全设置界面,选择“账户策略”→“账户锁定策略”菜单。双击“账户锁定阈值”选项,在弹出的对话框中输入允许尝试的最大登录次数,再单击“确定”按钮即可,如图 3.26 所示。

(18) 审核

进入“本地安全策略”→“本地策略”→“审核策略”,可见到以下项目内容:

审核策略更改成功,失败;
审核系统事件成功,失败;
审核账户登录事件成功,失败;
审核账户管理成功,失败.

对每一项目进行审核:双击每一项,选择成功(或失败),单击“确定”按钮完成设置,如图 3.27 所示。

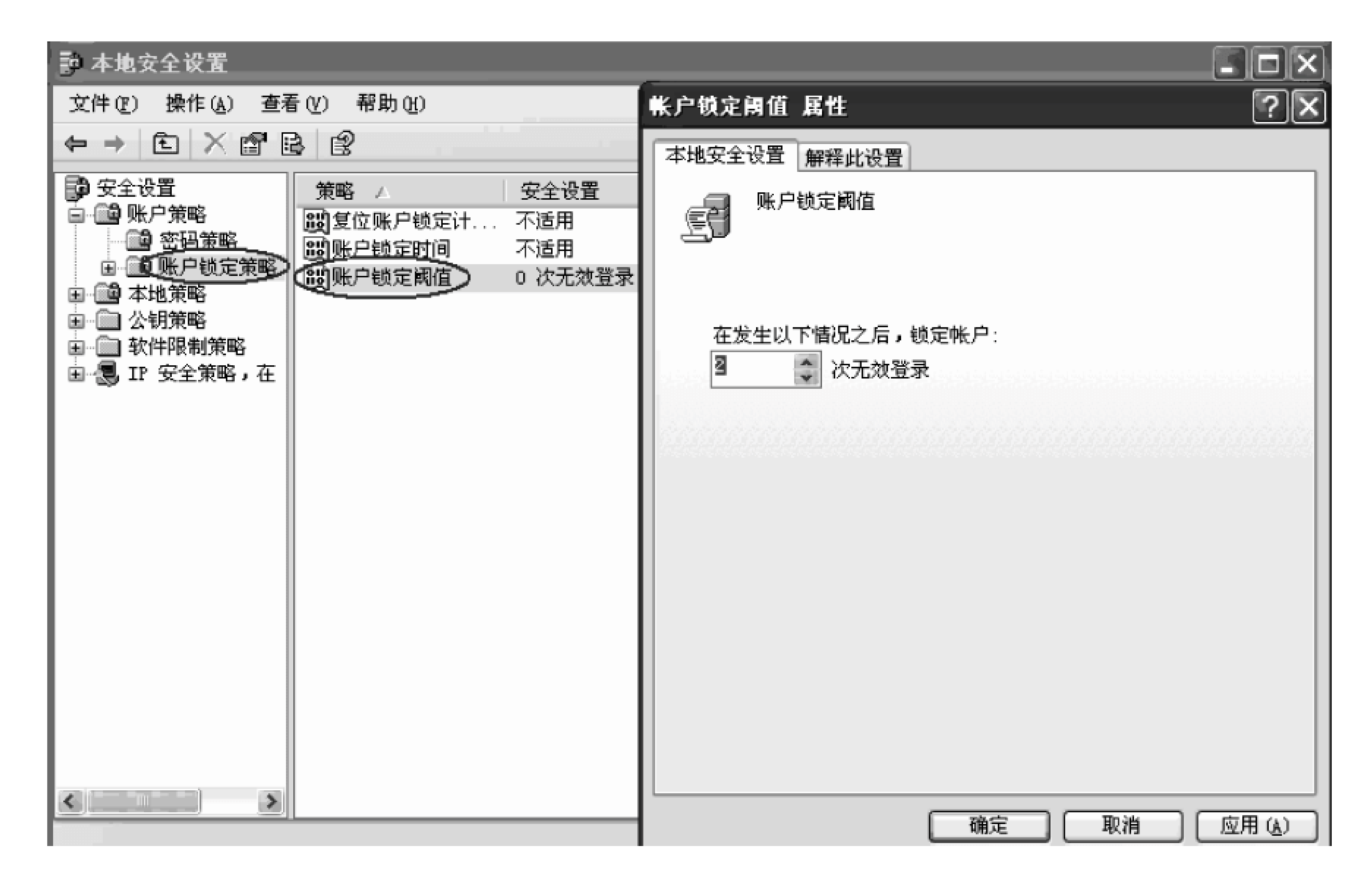


图 3.26　账户锁定设置



图 3.27　安全审核策略

3. 安全使用 Internet Explorer

Internet Explorer 是当今最流行的浏览器软件。因为使用的人多，IE 被发现的安全性问题也就最多。通过以下的设置，可以使 IE 更加安全。以下是以 IE 6.0 版为例介绍的，如果是其他版本，有些细节可能会有所差别。

(1) “Internet 选项”的“Internet”安全设置

打开 Internet Explorer，单击“工具”→“Internet 选项”菜单，打开“安全”选项卡。在“安全”菜单中选择“Internet”选项(见图 3.28)，就可以针对 Internet 区域的一些安全选项进行设置。虽然有不同级别的默认设置，但最好是根据自己的实际情况亲自调整一下。单击下方的“自定义级别”按钮，这里就显示了 IE 安全设置，如图 3.29 所示。

① 下载已签名的 Active X 控件：经过第三方的认证机构签名证明该 Active X 控件是安全的，并且可以设置为允许下载这种控件，除非不想安装任何 Active X 控件，或者想从一



图 3.28 Internet 选项的安全设置(1)



图 3.29 Internet 选项的安全设置(2)

些网站下载，例如 Windows Update，还有播放 Flash 的插件等。

② 下载未签名的 Active X 控件：与经过签名认证的 Active X 控件相比，未经签名认证的可能会包含潜在的安全隐患，因此该选项最好不要设置为启用，可设为“禁用”或者设置为“提示”，这样可以根据正在访问的站点的性质决定是否下载安装未经认证的控件。

③ 对没有标记为安全的 Active X 控件进行初始化和脚本运行：与前面的设置类似，如果之前都设置为“禁用”，那么该选项同样“禁用”即可，否则可以设置为“提示”或者“启用”，禁止那些未经签名的控件运行。

④ 运行 Active X 控件和插件：假设已经“禁止”了所有 Active X 控件和插件的运行，那么该选项就可以放心地设置为管理员认可。

⑤ 对标记为可安全执行脚本的 Active X 控件执行脚本：该设置可以与前面的选项相同。

⑥ 活动脚本：现在各种脚本程序非常流行，通过脚本程序可以建立很多实用的网页，例如 Windows Update 网页，就是通过脚本程序来判断需要下载的补丁。因此如果“禁用”脚本程序，一些网页将不能正常浏览，这里建议设置为“禁用”。

⑦ 允许通过脚本进行粘贴操作：该选项允许网页通过脚本把文件复制到剪贴板，为了安全考虑最好设为“禁用”。

⑧ Java 小程序脚本：JavaScript 是一种公开、多平台、面向对象的脚本语言。很多网页中都使用了 Java 脚本，但是安全起见最好“禁用”它。

(2)“Internet 选项”的“可信站点”安全设置

以上的设置会影响到少数必须要访问的站点(例如 Windows Update 网站)，但为了安全起见又不想把 Internet 区域的安全级别设置得太低，则可以把一些信任的站点添加到“受信任的站点”中去。方法是：在“Internet 选项”的“安全”选项卡下，单击“受信任的站点”，然后单击“站点”按钮，在新窗口中输入希望添加的网络地址(例如 http://www.163.com)，如图 3.30 所示，然后单击右侧的“添加”按钮即可。



图 3.30　Internet 选项的可信站点设置

(3)“Internet 选项”的“内容”安全设置

打开“Internet 选项”中的“内容”选项卡，可看到有“分级审查”、“证书”和“个人信息”三栏，如图 3.31 所示。

“分级审查”可以帮助用户控制在该计算机上看到的 Internet 内容。单击“分级审查”的“启用”按钮，弹出“内容审查程序”对话框，如图 3.32 所示。在这里可对内容的级别和可信站点进行查看和设置。

在“证书”栏，使用证书可以正确标识自己、证书颁发机构和颁发商的身份。单击“证书”按钮，弹出“证书”对话框，如图 3.33 所示。在该对话框中，可帮助个人用户将证书、证书信任列表和证书吊销列表从磁盘复制到证书存储区，可列出“中级证书颁发机构”、“受信任的



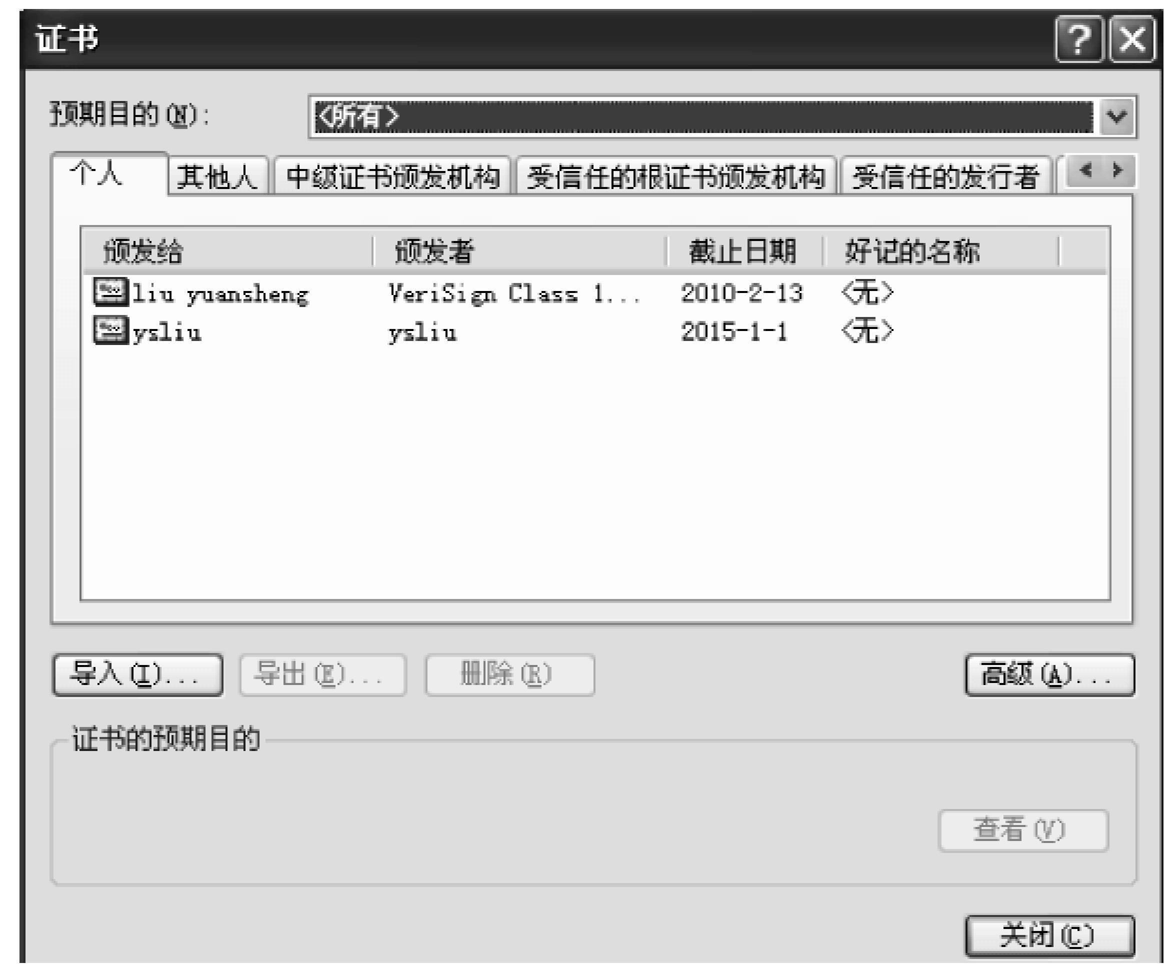
图 3.31 Internet 选项的“内容”设置

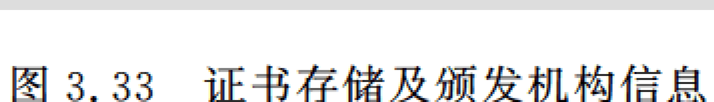


图 3.32 “分级审查”的“内容审查程序”对话框

根证书颁发机构”等相关信息。

在“个人信息”栏，单击“自动完成”按钮，弹出如图 3.34 所示的对话框。对于所列出来的每一项，自动完成功能都会保存特定的内容，其中“Web 地址”会保存在 IE 地址栏中输入过的内容；“表单”会保存在网页中填写的资料，例如论坛上的发言(除用户名和密码)、搜索引擎中使用过的关键字等；“表单上的用户名和密码”会保存登录论坛或其他网页时输入的用户名和密码。自动完成可以帮助节省很多时间，但是同时也带来了很大的安全隐患。一旦有人使用你的账号登录，登录网站的用户名和密码等资料就有可能全部被别人看到。因此用户可以根据自己的计算机使用情况适当调整，决定哪些内容可以自动保存，哪些不行。




图 3.33　证书存储及颁发机构信息

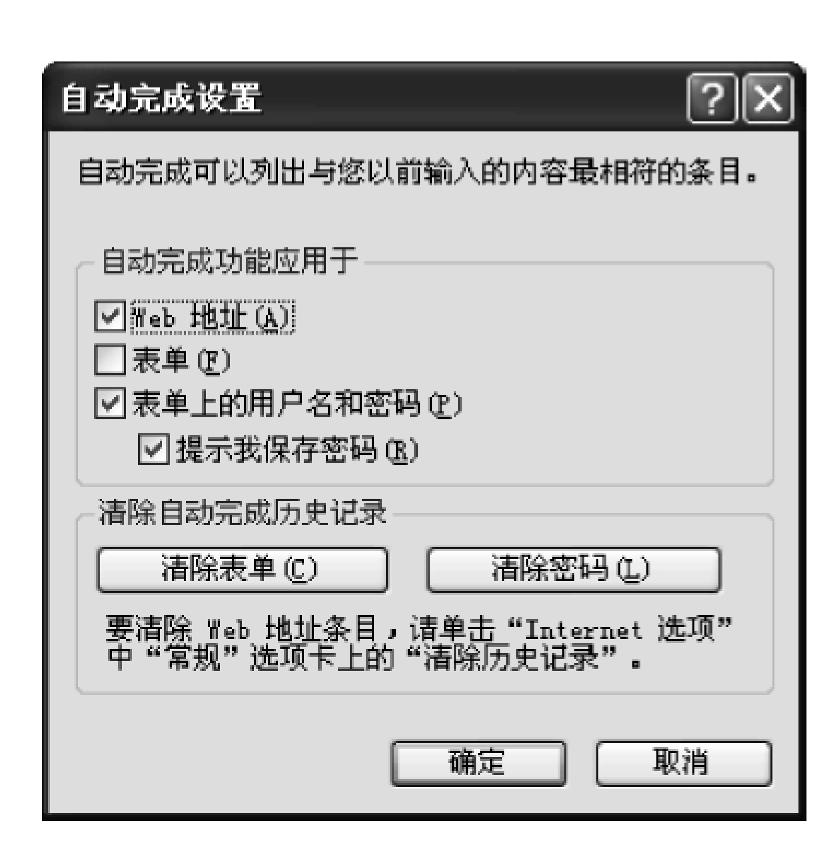


图 3.34　个人信息的"自动完成设置"对话框

(4)"Internet 选项"的"高级"安全设置

打开"Internet 选项"的"高级"选项卡，可根据实际情况对"设置"中的各"安全"项进行以下具体设置，如图 3.35 和图 3.36 所示。



图 3.35　Internet 选项的"高级"设置(1)



图 3.36　Internet 选项的"高级"设置(2)

① 检查发行商的证书吊销：如果选择了该项，当访问某些需要认证的站点时，IE 会首先检查给站点提供的证书是否依然有效。一般情况下，建议启用该设置。

② 检查服务器证书吊销(需要重启动)：该项将会使 IE 检查站点服务器的证书是否仍然有效，一般也应该启用该设置。

③ 检查下载的程序的签名：如果启用该设置，在下载了程序后 IE 会通过签名自动检查程序是否被非法改动过。一般应当启用该设置。

④ 不将加密的页面存入硬盘：启用了该项后，对于加密页面（主要是 URL 以 https 打头的）将不会保存到 Internet 临时文件夹中。如果多人共用同一台计算机，该选项是很有必要的，这样别人就无法通过 Internet 临时文件窥探到你访问过的加密网页了。

⑤ 对无效站点证书发出警告：启用该设置之后，在遇到无效的站点证书时 IE 就会发出警告，提醒注意。一般情况下可以启用该设置。

⑥ 在安全和非安全模式之间转换时发出警告：当启用该设置之后，如果要从一个安全的网页（可能是经过 SSL 加密的）进入到一个不安全的网页时，IE 会发出警告，以避免在不知情的情况下泄露一些私人的信息。

⑦ 重定向提交的表单时发出警告：启用该设置后，在某些论坛或类似的地方提交的一些信息如果被发送到了其他的服务器上，IE 就会发出警报。所以为安全起见，也应当启用该设置。

3.3.2 Linux 系统安全及服务器配置

人们普遍认为 Linux 比 Windows 安全，这是有道理的。因为 Windows 树大招风，这应该算是其中的一个原因吧。但 Linux 也不是绝对安全的，尤其是在默认设置情况下。本节介绍 Linux 系统的安全及基于 Linux 的服务器的安全设置。

1. BIOS 的安全设置

首先用户要给自己的 BIOS 设置密码，这是最基本的要求。这样可以防止通过在 BIOS 中改变启动顺序，而从软盘启动。这样可以阻止别人试图用特殊的启动盘启动你的系统，还可以阻止别人进入 BIOS 改动其中的设置，使机器的硬件设置不能被别人随意改动。

2. GRUB 安全设置

（1）设置全局口令锁定启动菜单

全局口令用于设置只允许用户选择启动菜单项进行启动。password 命令可为 GRUB 的启动菜单和菜单项设置口令，在 grub. conf 的全局配置部分使用 password，例如在第一个 title 上输入 password yaohoo。Linux 下用 vi/vim 命令来编辑，如输入命令“vi/boot/grub/grub. conf”，即可进入如图 3.37 所示编辑界面进行编辑。

```
root@yesir:~
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, e
g.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda3
#          initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password yaohoo
title CentOS (2.6.18-92.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-92.el5 ro root=LABEL=/ rhgb quiet
        initrd /initrd-2.6.18-92.el5.img
```

图 3.37　设置全局口令

设置全局口令后，GRUB 启动菜单被锁定，此时只允许选择菜单项进行启动。如需对菜单进行其他操作（如编辑、进入命令行界面等），都应先对启动菜单进行解锁。在锁定的启动菜单选“P”，输入口令解锁即可恢复正常的状态。

（2）使用全局口令锁定启动菜单

GRUB 提供了菜单项级别的保护。对于需要保护的菜单项，可以使用已设置的全局口令进行锁定。如果启动该菜单项需先输入全局口令对该菜单项进行解锁。设置步骤如下：

① 设置 GRUB 全局口令。

② 在菜单项配置中使用 lock 命令锁定菜单项，如图 3.38 所示。Lock 的作用是使用全局口令锁定某启动菜单项。该命令没有参数，一般紧跟 title。锁定启动菜单项中 lock 之后的所有命令，直到输入正确的口令。

```
root@yesir:~
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, e
g.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda3
#          initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password yaohoo
title CentOS (2.6.18-92.el5)
lock
        root (hd0,0)
        kernel /vmlinuz-2.6.18-92.el5 ro root=LABEL=/ rhgb quiet
-- INSERT --
```

图 3.38 使用 lock 命令锁定菜单项

当需要对不同启动菜单项使用不同的口令进行验证管理时，可以在各菜单项中使用独立的 password 设置，如图 3.39 所示。这样，就可以实现全局口令和菜单项口令的分级管理。如为某菜单项设置独立口令最好先设置全局口令，并确保口令字各不相同，如不设置全局口令会造成菜单项口令的泄露。

```
root@yesir:~
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, e
g.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda3
#          initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password yaohoo
title CentOS (2.6.18-92.el5)
password netyi
        root (hd0,0)
        kernel /vmlinuz-2.6.18-92.el5 ro root=LABEL=/ rhgb quiet
-- INSERT --
```

图 3.39 password 设置

（3）使用 MD5 加密口令

为了避免在配置文件中使用明文口令，可采用 MD5 加密口令，如图 3.40 所示。

```
root@yesir:~
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, e
g.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda3
#          initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$VB/Nc$9PyEDKiXZqReIZAEbXSAM1
title CentOS (2.6.18-92.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-92.el5 ro root=LABEL=/ rhgb quiet
        initrd /initrd-2.6.18-92.el5.img
```

图 3.40　采用 MD5 加密口令

（4）口令安全

口令可以说是系统的第一道防线，目前网上的大部分对系统的攻击都是从截获口令或者猜测口令开始的，所以应该选择更加安全的口令。

① 要杜绝不设口令的账号存在。这可以通过查看/etc/passwd 文件发现。如果用户名为 test 的账号没有设置口令，则在/etc/passwd 文件中就有

```
test ::100:9::/home/test:/bin/bash
```

该行的第二项为空，说明 test 账号没有设置口令，这是非常危险的，应将该类账号删除或者设置口令。

② 在旧版本的 Linux 中，/etc/passwd 文件中包含有加密的密码。这样会给系统的安全性带来很大的隐患，因为可以用暴力破解的方法来获得密码。可以使用命令

```
/usr/sbin/pwconv 或/usr/sbin/grpconv
```

建立/etc/shadow 或/etc/gshadow 文件，这样在/etc/passwd 文件中不再包含加密的密码，而是将密码放在/etc/shadow 文件中，该文件只有超级用户 root 可读。

③ 修改一些系统账号的 Shell 变量。一定不要为 uucp、ftp、news 及一些仅仅需要 FTP 功能的账号设置/bin/bash 或/bin/sh 等 Shell 变量。可以在/etc/passwd 中将其 Shell 变量置空，例如设为/bin/false 或/dev/null 等，也可以使用

```
usermod – s /dev/null username
```

命令更改 username 的 Shell 为/dev/null。这样使用这些账号就不能从 Telnet 远程登录到系统中来了。

④ 要修改默认的密码长度。在用户安装 Linux 时默认的密码长度是 5 个字节。但这似乎不够，应该再增加一些位数，比如把它设为 8 字节，如图 3.41 所示。修改最短密码长度需要编辑 login 程序的配置文件 login.defs(vi/etc/login.defs)。

（5）自动注销账号

UNIX/Linux 系统中 root 账户具有最高的权限。如果系统管理员在离开系统之前忘记注销 root 账户，那将会带来很大的安全隐患。因此，应该让系统自动注销该账号。这可

```
root@yesir:~
#MAIL_FILE      .mail

# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be
 used.
#       PASS_MIN_DAYS   Minimum number of days allowed between p
assword changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a pa
ssword expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
```

图 3.41　修改默认的密码长度

通过修改账户中“TMOUT”参数(如图 3.42 所示)来实现此功能。编辑系统的 profile 文件(vi /etc/profile,用/histsize\c 找到 HISTSIZE),在"HISTSIZE="后面加入

```
TMOUT = 300
```

TMOUT 是按秒计算的,这里的 300 表示 300 秒。这样,如果系统中登录的用户在 5 分钟内都没有动作,那么系统会自动注销这个账户。管理员也可以在个别用户的.bashrc 文件中添加该值,以便系统对该用户实行特殊的自动注销。

```
root@yesir:~
ulimit -S -c 0 > /dev/null 2>&1

if [ -x /usr/bin/id ]; then
        USER="`id -un`"
        LOGNAME=$USER
        MAIL="/var/spool/mail/$USER"
fi

HOSTNAME=`/bin/hostname`
HISTSIZE=1000
TMOUT=300

if [ -z "$INPUTRC" -a ! -f "$HOME/.inputrc" ]; then
    INPUTRC=/etc/inputrc
fi
```

图 3.42　设置账户 TMOUT 参数

改变该项设置后,必须先注销用户,再用该用户登录才能激活此功能。

(6) 取消普通用户的控制台访问权限

可采用 shutdown、reboot、halt 等命令取消普通用户的控制台访问权限,如:

```
# rm -f /etc/security/console.apps/halt
# rm -f /etc/security/console.apps/poweroff
# rm -f /etc/security/console.apps/reboot
# rm -f /etc/security/console.apps/shutdown
# rm -f /etc/security/console.apps/xserver (此时只有 root 能用 x)
```

(7) 取消并反安装所有不用的服务

在系统中取消并反安装所有不用的服务，就会减少很多风险。查看/etc/inetd.conf 文件，通过注释取消所有不需要的服务（在该服务项目之前加一个“#”），然后用 sighup 命令升级 inetd.conf 文件。

① 更改/etc/inetd.conf 权限为 600，只允许 root 来读写该文件。

```
# chmod 600 /etc/inetd.conf
```

② 确定/etc/inetd.conf 文件所有者为 root。

③ 编辑 /etc/inetd.conf 文件（vi /etc/inetd.conf），取消不需要的服务，如 ftp、telnet、shell、login、exec、talk、ntalk、imap、pop3、finger、auth 等。把不需要的服务关闭，可以使系统的危险性降低很多。

④ 给 inetd 进程发送一个 HUP 信号。

```
# killall -HUP inetd
```

⑤ 用 chattr 命令把/etc/inetd.conf 文件设为不可修改，这样就可以防止对 inetd.conf 的任何修改。

```
# chattr +i /etc/inetd.conf
```

唯一可以取消该属性的用户只有 root。如果要修改 inetd.conf 文件，首先要用下面命令取消不可修改属性，修改后再把它的性质改回不可修改的。

```
# chattr -i /etc/inetd.conf
```

(8) TCP_WRAPPERS

使用 TCP_WRAPPERS 可以使系统安全面对外部入侵。最好的策略就是阻止所有的主机（在/etc/hosts.deny 文件中加入 ALL：ALL@ALL，PARANOID）登录，然后再在/etc/hosts.allow 文件中加入所有允许访问的主机列表。

① 编辑 hosts.deny 文件（vi /etc/hosts.deny），加入如下一行

```
# Deny access to everyone ALL: ALL@ALL, PARANOID
```

这表明除非该地址包在允许访问的主机列表中，否则阻塞所有的服务和地址。

② 编辑 hosts.allow 文件（vi /etc/hosts.allow），加入允许访问的主机列表，比如

```
ftp: 202.54.15.99 foo.com
```

这里的 202.54.15.99 和 foo.com 是允许访问 FTP 服务的 IP 地址和主机名称。

③ tcpdchk 程序是 tcpd wrapper 设置的检查程序，可用来检查 tcp wrapper 设置，并报告发现的潜在和真实的问题。设置完毕，运行如下命令即可。

```
# tcpdchk
```

(9) 修改/etc/host.conf 文件

/etc/host.conf 说明了如何解析地址。编辑/etc/host.conf 文件（vi /etc/host.conf），加入如下命令：

```
# Lookup names via DNS first then fall back to /etc/hosts
    order bind,hosts
# We have machines with multiple IP addresses
    multi on
# Check for IP address spoofing
    nospoof on
```

上述第一项设置首先通过 DNS 解析 IP 地址，然后通过 hosts 文件解析；第二项设置检测/etc/hosts 文件中的主机是否拥有多个 IP 地址（比如有多个以太口网卡）；第三项设置说明要注意对本机未经许可的电子欺骗。

（10）禁止从不同的设备进行 root 登录

/etc/securetty 文件允许定义 root 用户可以从哪个 TTY 设备登录。用户可以编辑/etc/securetty 文件，在不允许登录的 TTY 设备前添加“#”标志，来禁止从该 TTY 设备进行 root 登录。如在/etc/inittab 文件中有如下设置：

```
# Run gettys in standard runlevels
    1:2345:respawn:/sbin/mingetty tty1
    2:2345:respawn:/sbin/mingetty tty2
    #3:2345:respawn:/sbin/mingetty tty3
    #4:2345:respawn:/sbin/mingetty tty4
    #5:2345:respawn:/sbin/mingetty tty5
    #6:2345:respawn:/sbin/mingetty tty6
```

系统默认可以使用 6 个控制台。而在 3、4、5、6 序号前面加上禁止注释标志“#”，表示禁止使用这 4 个控制台，而只有另两个控制台可供使用。然后重新启动 init 进程，改动即可生效。

（11）Shell logging Bash

Shell 在～/.bash_history（～/表示用户目录）文件中保存了 500 条使用过的命令，这样可以为用户在输入使用过的长命令提供方便。每个在系统中拥有账号的用户在他的目录下都有一个.bash_history 文件。bash shell 应该保存少量的命令，并且在每次用户注销时都把这些历史命令删除。

① /etc/profile 文件中的 HISTFILESIZE 和 HISTSIZE 行确定所有用户的.bash_history 文件中可以保存的旧命令条数。建议把/etc/profile 文件中的 HISTFILESIZE 和 HISTSIZE 的值设为一个较小的数，比如 30。编辑 profile 文件（vi/etc/profile），定义两个值如下：

```
HISTFILESIZE = 30
HISTSIZE = 30
```

这表示每个用户的“.bash_history”文件可以保存 30 条旧命令。

② 在/etc/skel/.bash_logout 文件中添加

```
rm -f $HOME/.bash_history
```

这样，当用户每次注销时，.bash_history 文件都会被删除。

编辑.bash_logout 文件（vi /etc/skel/.bash_logout），添加如下行：

```
rm -f $HOME/.bash_history
```

(12) 给/etc/rc.d/init.d 下的 script 文件设置权限

给执行或关闭启动时执行的程序的 script 文件设置权限。运行下一行命令,说明只有 root 才允许读、写、执行该目录下的 script 文件。

```
# chmod -R 700 /etc/rc.d/init.d/*
```

(13) 隐藏系统信息

在默认情况下登录到 Linux 系统时,将显示该 Linux 发行版的名称、版本、内核版本、服务器的名称。对于黑客来说这些信息足够它入侵系统的。因此,应将这些系统信息隐藏起来,只显示一个 login:提示符。

编辑/etc/rc.d/rc.local 文件,在下面各行前加一个#,把输出信息的命令隐藏起来。

```
# This will overwrite /etc/issue at every boot. So, make any changes you
    # want to make to /etc/issue here or you will lose them when you reboot
    #echo "" > /etc/issue
    #echo "$R" >> /etc/issue
    #echo "Kernel $(uname -r) on $a $(uname -m)" >> /etc/issue
    #
    #cp -f /etc/issue /etc/issue.net
    #echo >> /etc/issue
```

其次删除/etc 目录下的 issue.net 和 issue 文件:

```
# rm -f /etc/issue
# rm -f /etc/issue.net
```

习题和思考题

一、问答题

1. 常用的网络操作系统有哪些?
2. 什么是系统漏洞补丁? 其作用是什么?
3. 简述常用的访问控制措施。
4. 入网访问控制通常包括哪几方面?
5. 简述选择口令和保护口令的方法。
6. 简述 Windows 系统的漏洞。
7. 简述 Windows 2000/2003 系统新增加和改进的安全措施和技术。
8. 简述 Linux 系统的安全性。
9. 简述对一般用户账号的管理措施。

二、填空题

1. 网络访问控制可分为(　　)和(　　)两大类。

2. (　　)访问控制指由系统提供用户有权对自身所创建的访问对象进行访问,并可将对这些对象的访问权授予其他用户和从授予权限的用户收回其访问权限。

3. 常用的身份验证方法有用户名和口令验证、(　　)、Security ID 验证和(　　)等。

4. 网络操作系统的主要安全功能包括(　　)、文件保护、(　　)和(　　)等。

5. 入网访问控制主要就是对要进入系统的用户进行识别,并验证其合法身份。系统可以采用(　　)、(　　)和(　　)等方法实现入网访问控制。

6. 补丁程序是(　　)小程序。

7. 安装补丁程序的方法通常有(　　)和手工操作。

三、单项选择题

1. 网络访问控制可分为自主访问控制和强制访问控制两大类。(1)(　　)是指由系统对用户所创建的对象进行统一的限制性规定。(2)(　　)是指由系统提供用户有权对自身所创建的访问对象进行访问,并可将对这些对象的访问权授予其他用户和从授予权限的用户收回其访问权限。用户名/口令、权限安全、属性安全等都属于(3)(　　)。

(1) A. 服务器安全控制　　B. 检测和锁定控制
C. 自主访问控制　　D. 强制访问控制

(2) A. 服务器安全控制　　B. 检测和锁定控制
C. 自主访问控制　　D. 强制访问控制

(3) A. 服务器安全控制　　B. 检测和锁定控制
C. 自主访问控制　　D. 强制访问控制

2. 用户名/口令限制、账户锁定、身份认证、入网时间和端点地址等限制是系统访问控制中的(　　)安全措施。

A. 入网访问控制　　B. 用户权限　　C. 文件和目录属性　　D. 服务器保护

四、实验题

1. 利用系统的“本地连接”功能关闭不必要的端口。

2. 利用“组策略编辑器”或“本地安全策略”杜绝非法访问应用程序、关闭自动播放服务、删除默认共享、清空远程可访问的注册表路径、账户锁定设置、设置密码、安全审核。

3. 对 IE 进行安全设置。

第4章 数据加密技术与应用实践

随着信息技术的发展和计算机通信网络的广泛应用,世界正步入网络经济时代。对更有效的生产和产品销售渠道的需求,引发了人们对高技术生产力的要求,由此产生了一批具有代表性的网络经济模式,如电子商务(electronic commerce)、电子现金(electronic cash)、数字货币(digital cash)、网络银行(network bank)等。有专家预言,到2010年底,发生在Internet上的贸易金额将会达到100 000亿美元。

为了保障计算机网络的安全,需要采取严格的管理和各种先进技术。安全立法对保护网络系统安全有不可替代的重要作用,但依靠法律也阻止不了攻击者对网络数据的各种威胁。加强行政、人事管理,采取物理保护措施等都是保护系统安全不可缺少的有效措施,但有时这些措施也会受到各种环境、技术、费用以及系统工作人员素质等条件的限制。采用访问控制、系统软硬件保护等方法保护网络系统资源,简单易行,但也存在诸如系统内部某些职员可以轻松越过这些障碍而进行计算机犯罪等不易解决的问题。采用密码技术保护网络中存储和传输的数据,是一种非常实用、经济、有效的方法。对信息进行加密保护可以防止攻击者窃取网络机密信息,可以使系统信息不被无关人员识别,也可以检测出非法用户对数据的插入、删除、修改及滥用有效数据的各种行为。

本章主要介绍密码学基础、数据加密算法、数字签名和密钥管理等常用的数据保密技术和方法。

4.1 密码学基础

密码学(cryptography)是一门古老的学科,在古代就已经得到应用,但仅限于外交和军事等重要领域。随着现代计算机技术的飞速发展,密码技术正在不断向更多其他领域渗透。密码技术是保障信息安全的核心技术,是保证计算机网络安全的理论基础。

在计算机网络系统中,采用密码技术将信息隐蔽起来,再将隐蔽后的信息进行存储和传输。这样,即使信息在存储或传输过程中被窃取或截获,那些非法获得信息者因不了解这些信息的隐蔽规律,也就无法识别信息的内容,从而保证了计算机网络系统中的信息安全。

4.1.1 密码学的基本概念

1. 密码学简介

早在几千年前,人类就已经有了保密通信的思想和方法,但这些保密方法都是非常朴

素、原始和低级的，而且大多数是无规律的。有记载，最早的密码系统可能是希腊历史学家发明的 Polybios，这是一种替代密码系统。

到了 20 世纪 60 年代，随着电子技术、信息技术的发展及结构代数、可计算性理论和复杂度理论的研究，密码学又进入了一个新的时期。近年来，密码学研究之所以十分活跃，主要是它与计算机科学的蓬勃发展密切结合起来。此外，还有在电信、金融领域和防止日益广泛的计算机犯罪的需要。在 Internet 出现之前，密码技术已经广泛应用于军事和民用方面。现在，密码技术应用于计算机网络中的实例越来越多。

现代密码学是研究利用现代技术手段对计算机系统中的数据进行加密、解密和变换的学科，是数学和计算机科学交叉的学科，也是一门新兴的学科。随着计算机网络和现代通信技术的发展，现代密码学得到了前所未有的发展和应用。在国外，现代密码学已成为计算机系统安全的主要研究方向，也是计算机安全课程教学中的主要内容。

密码学包括密码编码学和密码分析学两部分。前者是研究密码变化的规律并用于编制密码，以保护秘密信息的科学，即研究如何通过编码技术来改变被保护信息的形式，使得编码后的信息除指定接收者之外的其他人都不能理解；后者是研究密码变化的规律并用于分析（解释）密码，以获取信息情报的科学，即研究如何攻破一个密码系统，恢复被隐藏起来的信息的本来面目。密码编码学是实现对信息保密的，密码分析学是实现对信息解密的，这两部分相辅相成，互相促进，也是矛盾的两个方面。

在 20 世纪 70 年代，密码学的研究出现了两大成果：一个是 1977 年美国国家标准局（NBS）颁布的联邦数据加密标准（DES）；另一个是 1976 年由 Diffie 和 Hellman 提出的公钥密码体制的新概念。DES 将传统的密码学发展到了一个新的高度，公钥密码体制的提出被公认为是实现现代密码学的基石。这两大成果已成为近代密码学发展史上两个重要的里程碑。

密码学是集数学、计算机、电子与通信等诸多学科于一身的交叉学科。它的主要任务是研究计算机系统和通信网络内信息的保护方法，以实现系统内信息的安全、保密、真实和完整。所以，使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和正确性，防止信息被篡改、伪造和假冒。随着计算机网络不断渗透到各个领域，密码学的应用范围也随之扩大。数字签名、身份验证等都是由密码学派生出来的新技术和应用。

2. 密码学的基本概念

(1) 加密与解密

在密码学中，通过使用某种算法并使用一种专门信息——密钥，将信息从一个可理解的明码形式变换成一个错乱的不可理解的密码形式，只有再使用密钥和相应的算法才能把密码还原成明码。

明文（plain text）也叫明码，是信息的原文，在网络中也叫报文（message），通常指待发的电文、编写的专用软件、源程序等，可用 P 或 M 表示。密文（cipher text）又叫密码，是明文经过变换后的信息，一般是难以识别的，可用 C 表示。

把明文变换成密文的过程就是加密（encryption），其反过程（把密文还原为明文）就是解密（decryption）。一般的密码系统模型如图 4.1 所示。

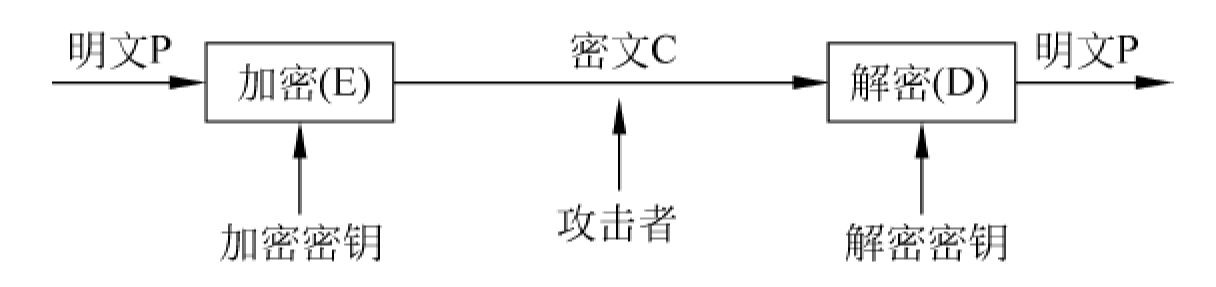


图 4.1 一般的密码系统示意图

密码算法(Algorithm)是加密和解密变换的一些公式、法则或程序,多数情况下是一些数学函数。密码算法规定了明文和密文之间的变换规则。加密时使用的算法称为加密算法,解密时使用的算法称为解密算法。

密钥(Key)是进行数据加密或解密时所使用的一种专门信息(工具),可看成是密码中的参数,用 K 表示。加密时使用的密钥称为加密密钥,解密时使用的密钥称为解密密钥。

密码系统是主要由密码算法和密钥组成的可进行加密和解密信息的系统。

数据加密过程就是利用加密密钥,对明文按照加密算法的规则进行变换,得到密文的过程。解密过程就是利用解密密钥,对密文按照解密算法的规则进行变换,得到明文的过程。

因为密码算法可以公开,也可以被分析,可以大量生产使用算法的产品,所有加密系统的安全性一般是基于密钥的安全性,而不是基于算法细节的安全性。只要破译者不知道你使用的密钥,他就对你的密码系统无能为力,就不能破译你的密文。

(2) 替代密码和移位密码

替代密码也称为置换密码。替代密码就是在加密时将明文中的每个或每组字符由另一个或另一组字符所替换,原字符被隐藏起来,即形成密文。

移位密码也称为换位密码。移位密码是在加密时只对明文字母(字符、符号)重新排序,每个字母位置变化了,但没被隐藏起来。移位密码是一种打乱原文顺序的加密方法。

替代密码加密过程是明文的字母位置不变而字母形式变化,移位密码加密是字母的形式不变而位置变化。

(3) 分组密码和序列密码

按明文加密时的处理过程划分,可分为分组密码和序列密码。

分组密码的加密过程是:首先将明文序列以固定长度进行分组,每组明文用相同的密钥和算法进行变换,得到一组密文。因此,可以说分组密码是以分组为单位,在密钥的控制下进行一系列线性和非线性变换而得到密文的。加密算法中重复地使用替代和移位两种基本的加密变换。分组密码具有良好的扩散性、对插入信息的敏感性高、较强的适应性、加密/解密速度慢、不需要密钥同步等特点。

序列密码的加密过程是:把报文、语音、图像等原始信息转换为明文数据序列,再将其与密钥序列进行“异或”运算,生成密文序列发送给接收者。接收者用相同的密钥序列与密文序列再进行逐位解密(异或),恢复明文序列。序列密码加/解密的密钥,可采用一个比特流发生器随机产生二进制比特流得到。这些随机比特流作为密钥,与明文结合产生密文,与密文结合产生明文。序列密码的安全性主要依赖于随机密钥序列。

(4) 对称密钥密码和非对称密钥密码

按加密和解密密钥的类型可分为对称密钥密码和非对称密钥密码。

加密和解密过程都是在密钥的作用下进行的。如果加密密钥和解密密钥相同或相近,

由其中一个很容易地得出另一个，这样的系统称为对称密钥密码系统。在这种系统中，加密和解密密钥都需要保密。对称密钥密码系统也称为单密钥密码系统或传统密钥密码系统。

如果加密密钥与解密密钥不同，且由其中一个不容易得到另一个，则这种密码系统是非对称密钥密码系统。这两个不同的密钥，往往其中一个是公开的，另一个是保密的。因此，非对称密钥密码系统也称为双密钥密码系统或公开密钥密码系统。

4.1.2 传统密码技术

数据的表示有多种形式，使用最多的是文字，其次还有图形、声音、图像等。传统加密方法加密的对象是文字信息。文字由字母组成，在字母表中 26 个英文字母是按顺序排列的，赋予它们相应的数字序号，如 A 对应序号 1，B 对应序号 2，…，Z 对应序号 26。因为大多数加密算法都有数学属性，这种表示方法便于对字母进行算术运算，因此可用数学方法进行加密变换。将字母表中的字母看做是循环的，将字母的加减运算变换为相应代码的算术运算，可用求模运算来表示（在标准的英文字母表中，模数为 26），如 A＋4＝E，X＋10＝H（因为 X 序号 24，24＋10＝34，34(mod 26)＝8，序号 8 对应的字母为“H”）。

1. 替代密码

替代密码在加密时将一个字母或一组字母的明文用另一个字母或一组字母替代，而得到密文。在传统密码学中，替代密码有简单替代、多字母替代和多表替代等类型。

简单替代密码也称为单表替代密码。简单替代就是将明文的一个字母，用相应的一个密文字母代替，规则是根据密钥形成一个新的字母表，与原明文字母表有相应的对应（映射）关系。简单替代加密方法有移位映射法、倒映射法和步长映射法等。简单替代密码很容易破译，因为它没有把明文不同字母出现的频率隐藏起来，所有密文都是由 26 个英文字母组成，字母出现的统计规律不变。破译这种密码的算法已经有很多种。

例 4-1 移位映射替代过程是用循环右移或循环左移一定位数的字符替代原字符的过程。如将英文字母按顺序循环右移 5 位进行替代，就可将 about 加密为 fgtzy，将 encryption 加密为 jshwduynts。

多字母替代密码的加密和解密都是将字母以块为单位进行的，比如，ABA 对应于 OST，ABB 对应于 STL。在第一次世界大战中，英国人就采用了这种对成组字母加密的密码。

多表替代密码是 19 世纪后期发明的，在美国南北战争期间由联军使用。多表替代密码是由多个简单替代密码构成。一种典型的多表替代密码叫 Vigenere（维吉尼亚）密码。

2. 移位密码

移位密码加密时只对明文字母重新排序，字母位置变化了，但它们没有被隐藏。移位密码加密是一种打乱原文顺序的替代法。

例 4-2 把明文“this is a bookmark”按行写出，分为三行五列，则成为以下形式：

t h i s i
s a b o o
k m a r k

读出时按从左到右的列顺序进行，可得到密文 tskhamibasoriok。该例的密钥就是

12345,即按列读出的顺序。

例 4-3 对上例还可以用另一种顺序选择相应的列输出得到密文。如用 china 为密钥,对 this is a bookmark 排列成上述矩阵。密钥 china 对应的序号为 23451,再以从小到大的顺序输出,即可得到密文 ioktskhamibasor。

例 4-4 对于句子"移位密码加密时只对明文字母重新排序字母位置变化但它们没被隐藏",可选择密钥"362415",并循环使用该密钥对上句进行换位加密。密钥的数字序列代表明文字符(汉字)在密文中的排列顺序。按照该密钥加密可得到一个不可理解的新句子(密文)"密密位码移加对字只明时文新字重排母序置但位变母化没藏们被它隐"。解密时只需按密钥 362415 的数字从小到大顺序将对应的密文字符排列,即可得到明文。

3. 一次一密钥密码

一次一密钥密码就是指每次都使用一个新的密钥进行加密,然后该密钥就被丢弃,下次再加密时再选择一个新密钥进行。一次一密钥密码是一种理想的加密方案。一次一密钥密码的密钥就像每页都印有密钥的簿子一样,称为一次一密密钥本,该密钥本就是一个包括多个随机密钥的密钥字母集,其中每一页上记录一条密钥。加密时使用一次一密密钥本的过程类似于日历的使用过程,每使用一个密钥加密一条信息后,就将该页撕掉作废,下次加密时再使用下一页的密钥。

发送者使用密钥本中每个密钥字母串去加密一条明文字母串,加密过程就是将明文字母串和密钥本中的密钥字母串进行模 26 加法运算。接收者有一个同样的密钥本,并依次使用密钥本上的每个密钥去解密密文的每个字母串。接收者在解密信息后也销毁密钥本中用过的一页密钥。

一次一密钥密码主要用于高度机密的低带宽信道。美国与前苏联之间的热线电话据说就是用一次一密密钥本加密的,许多前苏联间谍传递的信息也是用一次一密密钥本加密的。至今这些信息仍是保密的,并将一直保密下去。不管超级计算机工作多久,也不管有多少人用什么样的方法和技术,具有多大的计算能力,他们都不能阅读前苏联间谍用一次一密密钥本加密的信息,除非他们恰好回到那个年代,并得到加密信息的一次一密密钥本。

4.2 数据加密技术

4.2.1 对称密钥密码体制及算法

1. 对称密钥密码的概念

对称密钥密码体制也称为传统密钥密码体制,其基本思想就是"加密密钥和解密密钥相同或相近",由其中一个可推导出另一个。使用时两个密钥均需保密,因此该体制也称为单密钥密码体制。对称密钥密码体制模型如图 4.2 所示。

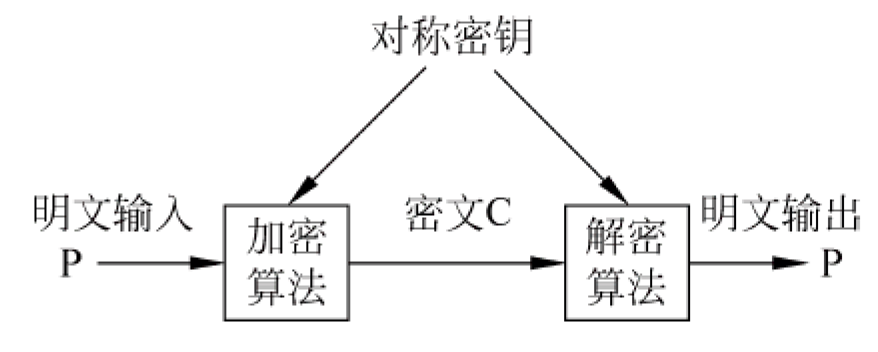


图 4.2 对称密钥密码体制模型

一个对称密钥密码体制的工作流程是:假定 A 和 B 是两个系统,二者决定进行保密通信。A 和

B 通过某种方式获得一个可共用的秘密密钥，该密钥只有 A 和 B 知道，其他用户都不知道。A 或 B 通过使用该密钥加密发送给对方的信息，收到后用已知的密钥解密，其他用户均无法解密该信息，这样就达到了信息传输的保密性目的。

2. 对称密钥密码算法

典型的对称密钥密码算法有 DES、TDEA(3DES)、IDEA、AES、MD5 等。

(1) DES 算法简介

数据加密标准(DES)是由 IBM 公司研制的，并经长时间论证和筛选后，于 1977 年由美国国家标准局颁布的一种加密算法。DES 主要用于民用敏感信息的加密，1981 年被国际标准化组织接纳为国际标准。DES 主要采用替换和移位的方法加密。它用 56 位密钥对 64 位二进制数据块进行加密，每次加密可对 64 位的输入数据进行 16 轮编码，经一系列替换和移位后，输入的 64 位原始数据就转换成了完全不同的 64 位输出数据。DES 算法仅使用最大为 64 位的标准算术和逻辑运算，运算速度快，密钥产生容易，适合于大多数计算机上用软件方法实现，同时也适合于在专用芯片上实现。

DES 算法能对 64 位二进制数码组成的数据组在 56 位密钥的控制下进行加密和解密，56 位密钥包含在 64 位密钥组中。图 4.3 是 DES 加密/解密算法示意图。DES 是一个对称算法，加密和解密使用同一算法，只是加密和解密时使用的子密钥顺序不同。

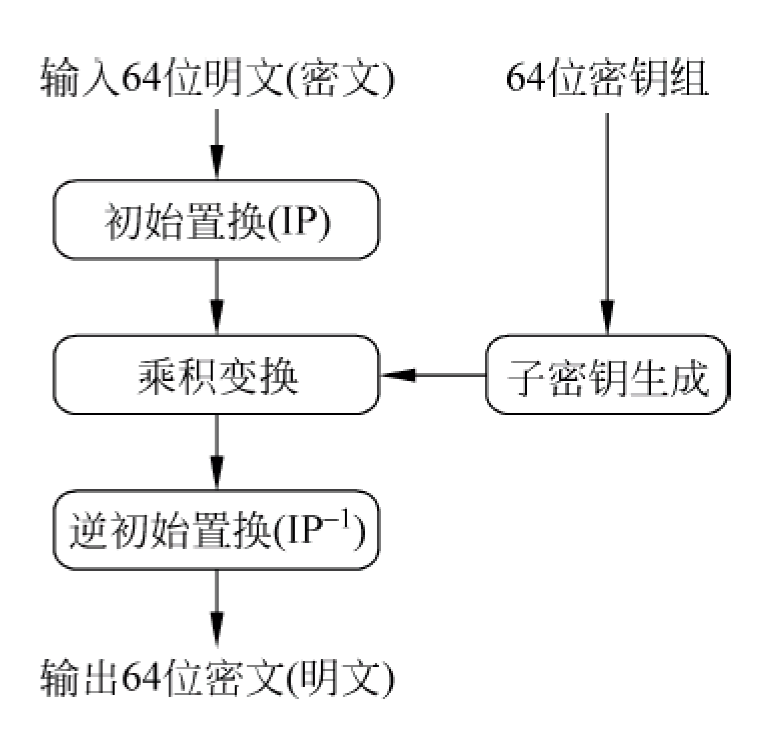


图 4.3　DES 算法流程略图

如图 4.3 所示，DES 算法是按下列四个主要过程实现的。图的左边是明文的处理过程，有 3 个阶段，右边是子密钥的生成过程。

- 子密钥生成：由 64 位外部输入密钥组通过置换选择和移位操作生成加密和解密所需的 16 组子密钥，每组 56 位。
- 初始置换(initial permutation，IP)：初始置换在第一轮运算之前进行，用来对输入的 64 位数据组进行换位变换，即按照规定的矩阵改变数据位的排列顺序。此过程是对输入的 64 位数据组进行的与密钥无关的变换。
- 乘积变换：该过程与密钥有关，它包括多次线性变换和非线性变换，且非常复杂，是加密过程的关键。它采用的是分组密码，通过 16 次重复的替代、移位、异或和置换来打乱原输入数据组。打乱了原输入数据组，加大了非规律性，增加了系统分析的难度。在使用计算机处理时，把大的数据组作为一个单元来进行变换，其优点是增加替代和重新排列方式的种类。
- 逆初始置换(IP^{-1})：逆初始置换(也称为末置换)是 DES 算法的最后一步，与初始置换处理过程相同，置换矩阵是初始置换的逆矩阵。逆初始置换是一次简单的数码换位，也是线性变换，该变换与密钥无关。

由于 DES 算法可用 56 位密钥组把 64 位明文(或密文)数据加密(或解密)成 64 位密文(或明文)数据组，故当 DES 算法作为一种标准算法公开的情况下，信息的秘密完全寓于 56 位密钥之中，因此如何选取密钥十分重要。

DES 是世界上使用最为广泛和流行的一种分组密码算法，被公认为世界上第一个实用的密码算法标准。它的出现适应了电子化和信息化的要求，也适合于硬件实现，因此该算法被制成专门的芯片，应用于加密机中。

DES 算法具有算法容易实现、速度快、通用性强等优点，但也存在密钥位数少，保密强度较差和密钥管理复杂的缺点。

DES 算法具体在 POS、ATM（自动取款机）、磁卡及智能卡（IC 卡）、加油站、高速公路收费站等领域被广泛应用，以此来实现关键数据的保密。如信用卡持卡人 PIN 的加密传输，IC 卡与 POS 间的双向认证、金融交易数据包的 MAC 校验等均可使用 DES 算法。

DES 在问世后的 20 多年里，成为密码界研究的重点，经受住了许多科学家的研究和破译，在民用密码领域得到了广泛的应用。它曾为全球贸易、金融等非官方部门提供了可靠的通信安全保障。DES 标准生效后，规定每隔 5 年由美国国家安全局 NSA（National Security Agency）进行一次评估，并确定它是否继续作为联邦加密标准使用。

DES 的缺点是密钥位数太短（56 位），而且算法是对称的，使得这些密钥中还存在一些弱密钥和半弱密钥，因此容易被采用穷尽密钥方法解密。此外，由于 DES 算法完全公开，其安全性完全依赖于对密钥的保护，必须有可靠的信道来分发密钥，如采用信使递送密钥等。因此，其密钥管理过程非常复杂，不适合在网络环境下单独使用，可以与非对称密钥算法混合使用。

(2) TDEA 算法简介

针对 DES 算法密钥短的问题，科学家提出在 DES 的基础上采用三重和双密钥加密的方法，这就是三重 DES 算法 TDEA（triple data encryption algorithm）。

TDEA 算法使用三个密钥，执行三次 DES 算法，如图 4.4 所示。加密过程为：

$$C = E_{K3}(D_{K2}(E_{K1}(M)))$$

解密时按密钥相反的顺序进行，可表述为：

$$M = D_{K1}(E_{K2}(D_{K3}(C)))$$

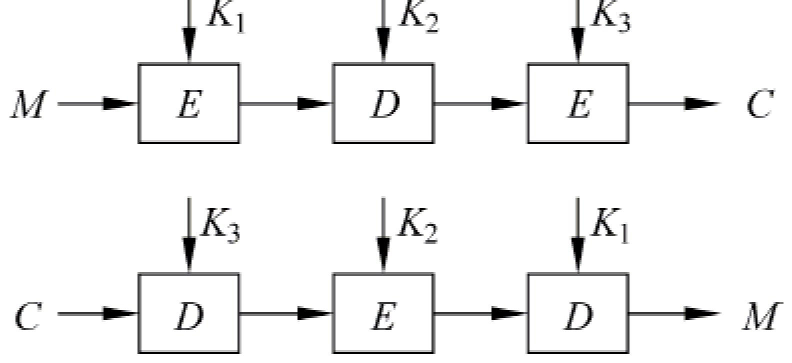


图 4.4　三重 DES 的加密解密过程

其中 M 表示明文，C 表示密文，$E_K(X)$ 表示使用密钥 K 对 X 进行加密，$D_K(X)$ 表示使用密钥 K 对密文 X 解密。

TDEA 算法使用两个 DES 密钥 K_1 和 K_2 进行三次 DES 的加密，其效果相当于将密钥长度增加一倍。

(3) IDEA 算法简介

国际数据加密算法（international data encryption algorithm，IDEA）是瑞士的著名学者提出的。IDEA 在 1990 年被正式公布并在以后得到增强。这种算法是在 DES 算法的基础上发展起来的，类似于三重 DES。发展 IDEA 也是因为 DES 存在密钥太短、容易被攻破等缺点。

IDEA 也是一种分组密码算法，分组长度为 64 位，但密钥长度为 128 位。该算法是用 128 位密钥对 64 位二进制码组成的数据组进行加密的，也可用同样的密钥对 64 位密文进行解密。

IDEA 与 DES 的明显区别在于循环函数和子密钥生成不同。对循环函数来说，IDEA

不使用 S 盒变换，而是依赖三种不同的数学运算：XOR、模 2^{16} 加法和模 $2^{16}+1$ 乘法运算。这些函数结合起来可以产生复杂的转换，这些转换很难进行密码分析。子密钥生成算法完全依赖于循环移位的应用，但使用方式复杂。

IDEA 算法设计了一系列加密轮次，每轮加密都使用从完整的加密密钥中生成的一个子密钥。每轮次中也使用压缩函数进行变换，只是不使用移位置换。IDEA 中使用的三种运算彼此混合可产生很好的效果。运算时 IDEA 把数据分为 4 个子分组，每个分组 16 位。

与 DES 的不同之处在于，IDEA 采用软件实现和硬件实现同样快速。IDEA 的密钥比 DES 的多一倍，增加了破译难度，被认为是多年后都有效的算法。

由于 IDEA 是在美国之外提出并发展起来的，避开了美国法律上对加密技术的诸多限制，因此，有关 IDEA 算法和实现技术的书籍都可以自由出版和交流，可极大地促进 IDEA 的发展和完善。

(4) AES 算法简介

高级加密标准(advanced encryption standard，AES)是由美国国家标准技术研究所 NIST 1997 年发起征集的数据加密标准，旨在得到一个非保密的、全球免费使用的分组加密算法，并能成为替代 DES 的数据加密标准。NIST 于 2000 年选择了比利时两位科学家提出的 Rijndael 作为 AES 的算法。

Rijndael 是一种分组长度和密钥长度都可变的分组密码算法，其分组长度和密钥长度分别为 128 位、192 位和 256 位。Rijndael 算法具有安全、高效和灵活等优点，使它成为 AES 最合适的选择。

① 安全性

Rijndael 算法的频数具有良好的随机特性，其密文比特服从 0.5 的二项式分布，因此其安全性大大增强。它对抗线性攻击和差分攻击的能力也很强。

② 高效性

由于 Rijndael 算法的线性和非线性混合层都采用矩阵运算，并且其变化的轮数(8～12 轮)较少，使得它具有很高的速度。

③ 灵活性

Rijndael 满足了 AES 的要求，密钥长度可为 128 位、192 位和 256 位，所以可根据不同的加密级别选择不同的密钥长度；其分组长度也是可变的，这正好弥补了 DES 的不足；其循环次数允许在一定范围内根据安全要求进行选取。这些都体现了该算法的灵活性。

4.2.2 公开密钥密码体制及算法

对称密钥加密方法是加密、解密使用同样的密钥，这些密钥由发送者和接收者分别保存，在加密和解密时使用。对称密钥方法的主要问题除密钥位数少、保密强度不够外，还有密钥管理(密钥的生成、管理、分发等)很复杂，特别是随着用户的增加，密钥的需求量成倍增加。如果网络中有 n 个用户，其中每两个用户之间都需要建立保密通信时，则系统中所需的密钥总数达 $n(n-1)/2$ 个，如果两个用户之间可能有多次通信，而每次通信的密钥又不能一样，这样网络中需要的密钥数又将大量增加。在网络通信中，大量密钥的分配和保管是一个很复杂的问题。

1. 公开密钥密码体制

美国斯坦福大学两名学者 W. Diffie 和 M. Hellman 1976 年在 IEEE Trans. on Information 刊物上发表了 *New Direction in Cryptography* 文章，提出了“公开密钥密码体制”的概念，开创了密码学研究的新方向。公开密钥密码体制的产生主要有两个方面的原因：一是由于对称密钥密码体制的密钥分配问题；另一个是由于对数字签名的需求。

与对称密钥加密方法不同，公开密钥密码系统采用两个不同的密钥对信息进行加密和解密。加密密钥与解密密钥不同，由其中一个不容易得到另一个。通常，在这种密码系统中，加密密钥是公开的，解密密钥是保密的，加密和解密算法都是公开的。每个用户有一个对外公开的加密密钥 K_e（称为公钥）和对外保密的解密密钥 K_d（称为私钥）。因此这种密码体制又称为非对称密码体制、公开密钥密码体制。

虽然解密密钥理论上可由加密密钥推算出来，但这种算法设计在实际上是不可能的；或虽然能够由加密算法推算出解密算法，但要花费很长时间因而使解密出的信息失去时效性变得毫无意义。所以，将加密密钥公开也不会危害解密密钥的安全。公开密钥加密算法和解密算法都是公开的。虽然保密密钥是由公开密钥决定的，但却不能由公开密钥计算出来。

自公钥加密体制问世以来，学者们提出了许多种公钥加密方法，如 RSA、背包算法、ElGamal、Rabin、DH 等，它们的安全性都是基于复杂的数学难题。根据所基于的数学难题来区分，有以下三类系统算法目前被认为是安全和有效的：大整数因子分解系统（代表性算法是 RSA）、椭圆曲线离散对数系统（ECC）和离散对数系统（代表性算法是 DSA）。

当前最著名、应用最广泛的公钥系统的密码算法是 RSA，它的安全性是基于大整数因子分解的困难性，而大整数因子分解问题是数学上的著名难题，至今没有有效的方法予以解决，因此可以确保 RSA 算法的安全性。

椭圆曲线加密算法（elliptic curve cryptography，ECC）是基于离散对数计算的困难性。ECC 与 RSA 方法相比，具有安全性能更高、运算量小、处理速度快、占用存储空间小、带宽要求低等优点。因此，ECC 系统是一种安全性更高、算法实现性能更好的公钥系统。

数字签名算法（data signature algorithm，DSA）是基于离散对数问题的数字签名标准，它仅提供数字签名功能，不提供数据加密功能。

2. RSA 算法简介

（1）RSA 算法

RSA 是由美国 MIT 的 3 位科学家 Rivest、Shamir 和 Adleman 于 1976 年提出的，故命名 RSA，并在 1978 年正式发表。RSA 系统是公钥系统的最具有典型意义的方法，大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是 RSA 算法。RSA 算法的优点主要在于原理简单，易于使用。RSA 是建立在素数理论（Euler 函数和欧几里得定理）基础上的算法。

在此不介绍 RSA 的理论基础（复杂的数学分析和理论推导），只简单介绍密钥的选取和加、解密的实现过程。

假设用户 *A* 在系统中要进行数据加密和解密，则可根据以下步骤选择密钥和进行加/

解密变换：

① 随机地选取两个不同的大素数 p 和 q（一般为 100 位以上的十进制数）予以保密。

② 计算 $n = p \cdot q$，作为 A 的公开模数。

③ 计算 Euler 函数

$$\Phi(n) = (p-1) \cdot (q-1) (\bmod\ n)$$

④ 随机地选取一个与 $(p-1) \cdot (q-1)$ 互素的整数 e，作为 A 的公开密钥。

⑤ 用欧几里得算法，计算满足同余方程

$$e \cdot d \equiv 1\ (\bmod\ \Phi(n))$$

的解 d，作为 A 的保密密钥。

⑥ 任何向 A 发送明文 M 的用户，均可用 A 的公开密钥 e 和公开模数 n，根据式

$$C = M^e (\bmod\ n)$$

得到密文 C。

⑦ 用户 A 收到 C 后，可利用自己的保密密钥 d，根据

$$M = C^d (\bmod\ n)$$

得到明文 M。

(2) RSA 算法举例

RSA 算法为公用网络上信息的加密和验证提供了一种基本的方法。它通常是先生成一对 RSA 密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。假设 B 要接收 A 的保密消息，则要生成私钥(D)和公钥(E)，然后将公钥和数字 N 发给 A。A 用 E 和 N 加密消息，然后将加密的消息发给 B。B 用私钥(D)解密消息。

例 4-5 对明文“18”进行加密、传输和解密。

① 选密钥

选择两个素数 $p=3, q=7$；则 $n=p \times q=3 \times 7=21$；因此得，$\Phi(n)=12$。

选择公钥（加密密钥）$e=5$，因 $5d \equiv 1(\bmod\ 12)$，可得私钥 $d=17$。

② 加密

明文 $M=18$，对其加密得到密文

$$C = 18^5 = 9\ (\bmod\ 21)$$

③ 传输

将密文 C 发送到接收方，接收方收到密文 $C=9$。

④ 解密

接收方可对密文进行解密，得到明文

$$M = 9^{17} = 18\ (\bmod\ 21)$$

例 4-6 对明文“HI”进行加密再解密。

① 选密钥

设 $p=5, q=11$，则 $n=55$，$\Phi(n)=40$。

取 $e=3$（公钥），则可得私钥 $d=27\ (\bmod\ 40)$。

② 加密

设明文编码为：空格=00，A=01，B=02，…，Z=26，则明文 HI=0809

$$C_1 = (08)^3 = 512 \equiv 17 \pmod{55}$$
$$C_2 = (09)^3 = 729 \equiv 14 \pmod{55}$$

因为 $Q=17$，$N=14$，所以，“HI”的密文为“QN”。

③ 解密

$$M_1 = C^d = (17)^{27} \equiv 08 \pmod{55}$$
$$M_2 = C^d = (14)^{27} \equiv 09 \pmod{55}$$

因为 $H=08$，$I=09$，所以，明文为“HI”。

(3) RSA 算法的特点及应用

RSA 算法具有密钥管理简单(网上每个用户仅保密一个密钥，且不需密钥配送)、便于数字签名、可靠性较高(取决于分解大素数的难易程度)等优点，但也具有算法复杂、加密/解密速度慢、难于用硬件实现等缺点。因此，公钥密码体制通常被用来加密关键性的、核心的、少量的机密信息，而对于大量要加密的数据通常采用对称密码算法。

RSA 算法的安全性建立在难于对大整数提取因子的基础上，研究表明大整数因式分解问题是一个极其困难的问题。但是，随着分解大整数方法的进步及完善、计算机速度的提高以及计算机网络的发展，对 RSA 加密/解密安全保障的大整数要求越来越大。当 n 足够大时(p 和 q 各为 100 位时，n 为 200 位)，对其进行分解就很困难了。可以说，RSA 的保密强度等价于分解 n 的难易程度。

4.3 数字签名技术及应用

4.3.1 数字签名的基本概念

网络安全系统一个很重要的方面是防止非法用户对系统的主动攻击，如伪造信息、篡改信息等。这种安全要求对实际网络系统的应用(如电子商务)是非常重要的。以下介绍的数字签名和验证都是基于数据加密的应用技术。

验证(authentication，也叫鉴别)是防止主动攻击的重要技术。验证的目的就是确认用户身份的合法性和用户间传输信息的完整性与真实性。验证服务主要包括报文验证和身份验证两方面。报文验证和身份验证可采用数据加密技术、数字签名技术及其他相关技术来实现。

报文验证是为了确保数据的完整性和真实性，对报文的来源、时间性及目的地进行验证。报文验证过程通常涉及加密和密钥交换。加密可使用对称密钥体制、非对称密钥体制或两种体制的混合方式进行。

身份验证就是验证申请进入网络系统者是否是合法用户，以防止非法用户访问系统。身份验证的方式一般有用户口令验证、摘要算法验证、基于 PKI(公钥基础设施)的验证等。

1. 身份验证

身份验证一般涉及两个过程：一个是识别；一个是验证。

识别是指要明确访问者是谁，即要对网络中的每个合法用户都有识别能力。要保证识

别的有效性,必须保证代表用户身份的识别符的唯一性。

验证就是指在访问者声明自己的身份后,系统要对他所申明的身份进行验证,以防假冒。

识别信息一般是非秘密的,如用户信用卡的号码、用户名、身份证号码等;而验证信息一般是秘密的,如用户信用卡的密码。

身份验证的方法有口令验证、个人持证验证和个人特征验证三类。

(1) 口令验证法最简单,系统开销也小,但其安全性最差。

(2) 持证为个人持有物,如钥匙、磁卡、智能卡等。持证法比口令法安全性好,但验证系统比较复杂。磁卡常和 PIN 一起使用。

(3) 以个人特征进行验证时,需要多种技术为验证机制提供支持,如指纹识别、声音识别、血型识别、视网膜识别等。个人特征方法验证的安全性最好,但验证系统也最复杂。

2. 数字签名

数字签名(digital signature)可解决手写签名中的签字人否认签字或其他人伪造签字等问题。因此,被广泛用于银行的信用卡系统、电子商务系统、电子邮件以及其他需要验证、核对信息真伪的系统中。

手工签名是模拟的,因人而异;而数字签名是数字式的(0、1 数字串),因信息而异。

数字签名具有以下功能。

(1) 接收方能够确认发方的签名,但不能伪造。

(2) 发送方发出签过名的信息后,不能再否认。

(3) 接收方对收到的签名信息也不能否认。

(4) 一旦收发双方出现争执,仲裁者可有充足的证据进行评判。

数字签名的目的是使报文的接收方能够对公正的第三方证明其报文内容是真实的,而且是由指定的发送方发出的。双方都不能出于自己的利益否认或修改报文的内容。签名所保护的内容可能会被破坏,但不会被欺骗。

数字签名基本形式是基于特定的附加信息的信息摘要。数字签名保证信息完整性的原理是:将要传送的明文通过一种单向散列函数运算转换成信息摘要(不同的明文对应不同的摘要),信息摘要加密后与明文一起传送给接收方,接收方对接收的明文进行计算产生新的信息摘要,再将其与发送方发来的信息摘要相比较。若比较结果一致,则表示明文未被改动,信息是完整的;否则,表示明文被篡改,信息的完整性受到破坏。

3. 单向散列函数

在现阶段,一般存在两个方向的加密方式,即双向加密和单向加密。

双向加密是加密算法中最常用的,它将可理解的明文数据加密成不可理解的密文数据;在需要的时候,再使用一定的算法和工具将这些密文解密为原来的明文。双向加密适合于保密通信,比如,在网上购物的时候,需要向网站提交信用卡密码。人们当然不希望自己的数据直接在网上明文传送,因为这样很可能被别的用户“偷听”,而希望自己的信用卡密码通过加密后再在网络传送。这样,网站接受到用户的数据后,通过解密算法就可以得到准确的信用卡账号。

单向加密是只对数据进行加密而不进行解密，即在加密后，不能对加密后的数据进行解密，或也不用再解密。单向加密算法用于不需要对信息解密或读取的场合。这种单向加密算法在实际中的典型应用就是对数据库中的用户信息进行加密，比如当用户创建一个新的账号及密码时，先将这些信息经过单向加密后再保存到数据库中。再比如，一台自动取款机(ATM)不需要解密一个消费者的个人标识号(PIN)，磁条卡将顾客的代码单向地加密成一段 Hash 值，使用时 ATM 机将计算用户 PIN 的 Hash 值并产生一个结果，然后再将这段结果与用户卡上的 Hash 值比较。使用这种方法，即使对于那些管理和维护 ATM 机的人来说，PIN 也是安全的。

Hash 函数就是一类单向加密数据的函数，也叫单向散列函数。目前已经有许多不同的 Hash 函数，在开放式网络系统中使用的安全性好的 Hash 函数如下：

(1) 基于分组密码算法的 Hash 函数。

(2) 系列 Hash 函数 MD2(信息摘要算法 2)、MD4 和 MD5 等，这些函数都产生 128 位的输出，MD5 就是一种优秀的单向加密算法。

(3) 美国政府的安全 Hash 标准(SHA-1)。SHA-1 是 MD4 的一个变形，产生 160 位的输出，与 DSA(数字签名算法)匹配使用。

4.3.2 数字签名标准

1. 数字签名与加密

对文件进行加密只解决传送信息的保密问题，而防止他人对传输的文件进行破坏，以及如何确定发信人的身份等还需要数字签名技术。在电子商务系统中，其安全服务都要用到数字签名技术。因此数字签名技术有着特别重要的地位。在电子商务中，完善的数字签名应具备签名方不能抵赖、他人不能伪造、在公证人面前能够验证真伪的能力。

一个由公开密钥密码体制实现的数字签名过程如图 4.5 所示。发送方 A 用自己的私钥 K_{Ad} 对明文信息 M 进行操作，使明文打上了 A 的标记得到签名信息 S；接收方 B 收到 S 信息后，用 A 的公钥 K_{Ae} 对 S 进行操作，即可得到原明文信息 M。

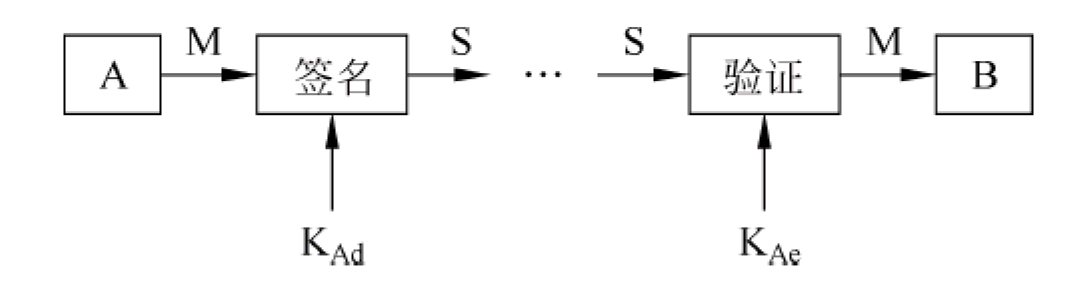


图 4.5 公钥体制实现数字签名的过程

数字签名的特点是它代表了文件的特征，文件如果发生改变，数字签名的值也将发生变化。不同的文件将得到不同的数字签名。一个最简单的 Hash 函数是把文件的二进制码相累加，取最后的若干位。Hash 函数对发收数据的双方都是公开的。

目前的数字签名大多是建立在公开密钥体制基础上，这是公开密钥加密技术的另一种重要应用。如基于 RSA 的公开密钥加密标准 PKCS、数字签名算法 DSA、PGP 加密软件等。

2. 数字签名算法

目前，广泛应用的数字签名算法主要有三种：RSA 签名、DSS(数字签名系统)/DSA(数字签名算法)签名和 Hash 签名。这三种算法可单独使用，也可结合在一起使用。

(1) RSA 算法签名

用 RSA 或其他公开密钥密码算法的最大方便是没有密钥分配问题(网络越复杂、网络用户越多，其优点越明显)。实际上 RSA 算法中的数字签名就是通过一个 Hash 函数来实现的。

采用 RSA 签名时，将消息输入到一个 Hash 函数以产生一个固定长度的安全 Hash 值，再用发方的私钥加密 Hash 值就形成了对消息的签名。消息及其签名被一起发给收方，收方得到消息后再产生出消息的 Hash 值，且使用发方的公钥对收到的签名解密。这样收方就得了两个 Hash 值，如果这两个 Hash 值是一样的，则认为收到的签名是有效的。

(2) DSS/DSA 签名

DSS/DSA 签名是由美国国家标准化研究院和国家安全局共同开发的。由于它是由美国政府颁布实施的，美国政府出于保护国家利益的目的不提倡使用任何削弱政府的有窃听能力的加密软件，因此，DSS/DSA 主要用于与美国政府做生意的公司，其他公司则较少使用。

DSS/DSA 的设计思想：签名者的计算能力较低且计算时间要短，而验证者计算能力较强。DSA 是在 ElGamal 和 Schnorr 两个签名方案基础上设计的，其安全性基于求离散对数的困难性。

DSA 是基于整数有限域离散对数难题的，其安全性与 RSA 相比差不多。DSA 的一个重要特点是两个素数公开，这样，当使用别人的 p 和 q 时，即使不知道私钥，也能确认它们是随机产生的，还是做了手脚。RSA 算法却做不到。

(3) Hash 数字签名

Hash 签名是最主要的数字签名方法，也称之为数字摘要法或数字指纹法。著名的数字摘要加密方法 MD5 由 RonRivest 所设计，该编码算法采用单向 Hash 函数将需加密的明文“摘要”成一串 128 位的密文。这样，该摘要就可成为验证明文是否“真实”的依据。

Hash 函数可产生信息摘要，其计算过程为：输入一个长度不固定的字符串，返回一串固定长度的字符串，即摘要，又称 Hash 值。信息摘要简要地描述了一份较长的信息或文件，它可以被看做一份长文件的“数字指纹”。信息摘要用于创建数字签名，对于特定的文件而言，信息摘要是唯一的。信息摘要可以被公开，它不会透露相应文件的任何内容。

Hash 函数主要可以解决两个问题：一是在某一特定的时间内，无法查找经 Hash 操作后生成特定 Hash 值的原报文；二是无法查找两个经 Hash 操作后生成相同 Hash 值的不同报文。这样，在数字签名中就可以解决签名验证、用户身份验证和不可抵赖性的问题。

Hash 函数除了可在数字签名中用来提高数字签名的有效性和分离保密与签名外，还可用于验证、数据完整性测试和加密。

3. 数字签名过程

数字签名的主要过程是：报文的发送方利用单向散列函数从报文文本中生成一个 128

位的散列值(或信息摘要)。发送方用自己的私钥对这个散列值进行加密来形成发送方的数字签名。然后,该数字签名将作为报文的附件和报文一起发送给报文的接收方。接收方首先从接收到的原始报文中计算出128位的散列值(或信息摘要),然后再用发送方的公开密钥对报文附加的数字签名进行解密得到原散列值。如果这两个散列值相同,则接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别。

采用数字签名能确认以下两点:第一,信息是由签名者发送的;第二,信息自签发到收到为止未曾做过任何修改。这样数字签名就可用来防止电子信息因易被修改而有人作伪,或冒用别人名义发送信息,或发出(收到)信件后又加以否认等情况发生。

只有加入数字签名及验证才能真正实现信息在公开网络上的安全传输。加入数字签名和验证的文件传输过程如下:

(1) 发送方首先用Hash函数从原报文中得到数字签名,然后采用公开密钥算法用自己的私钥对数字签名进行加密,并把加密后的数字签名附加在要发送的报文后面。

(2) 发送方选择一个会话密钥对原报文进行加密,并把加密后的文件通过网络传输到接收方。

(3) 发送方用接收方的公开密钥对会话密钥进行加密,并通过网络把加密后的会话密钥传输到接收方。

(4) 接收方使用自己的私钥对会话密钥信息进行解密,得到会话密钥的明文。

(5) 接收方用会话密钥对加密了的报文进行解密,得到原报文。

(6) 接收方用发送方的公开密钥对加密的数字签名进行解密,得到数字签名的明文。

(7) 接收方用得到的原报文和Hash函数重新计算数字签名,并与解密后的数字签名进行对比。如果两者相同,说明文件在传输过程中没有被破坏,信息完整。

如果第三方冒充发送方发出了一个文件,因为接收方在对数字签名进行解密时使用的是发送方的公开密钥,只要第三方不知道发送方的私钥,解密出来的数字签名和经过计算的数字签名必然是不同的。这就提供了一个安全的确认发送方身份的方法。

4.4 数据加密技术应用实例

本节介绍几种加密技术的应用实例,包括PGP软件、CA认证及数字证书、简单文档的加密应用,有关EFS、Kerberos和IPSec的加密应用在第5章中介绍。

4.4.1 加密软件PGP及其应用

1. PGP简介

PGP(pretty good privacy)是一个公钥加密程序。在传统的加密方法中,通常一个密钥既能加密也能解密。那么在开始传输数据前,如何通过一个不安全的信道传输密钥呢?使用PGP公钥加密法,用户可以广泛传播公钥,同时安全地保存好私钥。由于只有你可拥有私钥,所以,任何人都可以用你的公钥加密写给你的信息,而不用担心信息被窃听。

使用PGP的另一个好处是可以在文档中使用数字签名。一个使用私钥加密的文件只能用公钥解密。这样,如果人们阅读用你的公钥解密后的文件,他们就会确定只有你才能写

出这个文件。

PGP 把 RSA 公钥体系的密钥管理方便和传统加密体系的高速度结合起来，并且在数字签名和密钥认证管理机制上有巧妙的设计。虽然 PGP 主要是基于公钥加密体系的，但它不是一种完全的公钥加密体系，而是一种混合加密算法。它是由一个对称加密算法（IDEA）、一个非对称加密算法（RSA）、一个单向散列算法（MD5）和一个随机数产生器组成的，每种算法都是 PGP 不可分割的组成部分。PGP 之所以得到流行，得到大家的认可，最主要是它集中了几种加密算法的优点，使它们彼此得到互补。PGP 实现了目前大部分流行的加密和认证算法，如 DES、IDEA、RSA 及 MD5、SHA 等算法。

PGP 软件兼有加密和签名两种功能。它不但可以对用户的邮件保密，以防止非授权者阅读，还能对邮件进行数字签名，使收信人确信邮件未被第三者篡改。在 PGP 中，主要使用 IDEA 算法对数据进行加密（因为它速度快，安全性好）；使用 RSA 算法对 IDEA 的密钥进行加密（因为 RSA 公钥算法的密钥管理方便）。这样，两类体制的算法结合在一起实现加密功能，突出了各自的优点。PGP 还使用 MD5 作为散列函数，对数据的完整性进行保护，并与加密算法结合，提供数字签名功能。PGP 的加密功能和签名功能可以单独使用，也可以同时使用。

PGP 还可以只签名而不加密，这适用于用户发布公开的情况。用户为了证实自己的身份，在发送信件时用自己的私钥签名。这样就可以让收信人能确认发信人的身份，也可以防止发信人进行抵赖，这一点在商业领域有很大的应用前途。

对 PGP 来说，公钥本来就是公开的，不存在防偷盗问题，但公钥在发布中仍然存在被篡改和冒充的问题。PGP 对该问题采用 CA（权威机构）认证方法解决；而私钥相对于公钥而言不存在被篡改的问题，但却存在泄露的问题。对此，PGP 的解决办法是让用户为随机生成的 RSA 私钥指定一个口令，只有通过增加口令才能将私钥释放出来使用，保护私钥安全的问题实际上是对用户口令的保密。

2. PGP 的应用实例

PGP 可以用来对文件或邮件进行加密，以防止非授权者阅读。它还能对用户的文件或邮件加上数字签名，从而可以让收件人能确认发信人的身份，也可以防止发信人的抵赖行为。

（1）PGP 软件的下载与安装

在网上很多站点都可以自由下载到免费版本的 PGP 软件，比较权威的地址是 http://www.pgpi.org。现在网上免费的 PGP 新版本也很多，但有些还不太成熟和稳定。这里仍以较权威和稳定的 PGP 8.0.2 全免费版本为例介绍其应用。

从 http://www.pgpi.org 上下载 PGP 8.0.2，其容量约为 10MB。下载后单击安装文件开始安装。弹出 Welcome 界面、文档说明和 ReadMe 等窗口。随后可按提示输入用户名和机构名，选择安装路径。如果你是第一次使用 PGP，则在如图 4.6 所示对话框中选择“No，I'm a New User”选项。接下来一路确认（单击 Yes 或 Next 按钮）即可。安装完毕后按要求重新启动系统，如图 4.7 所示（系统会自动缩为托盘上的一个小锁头图标）。

（2）选取密钥

PGP 使用 IDEA 算法加密数据，IDEA 的密钥使用 RSA 或 DH 算法进行加密。

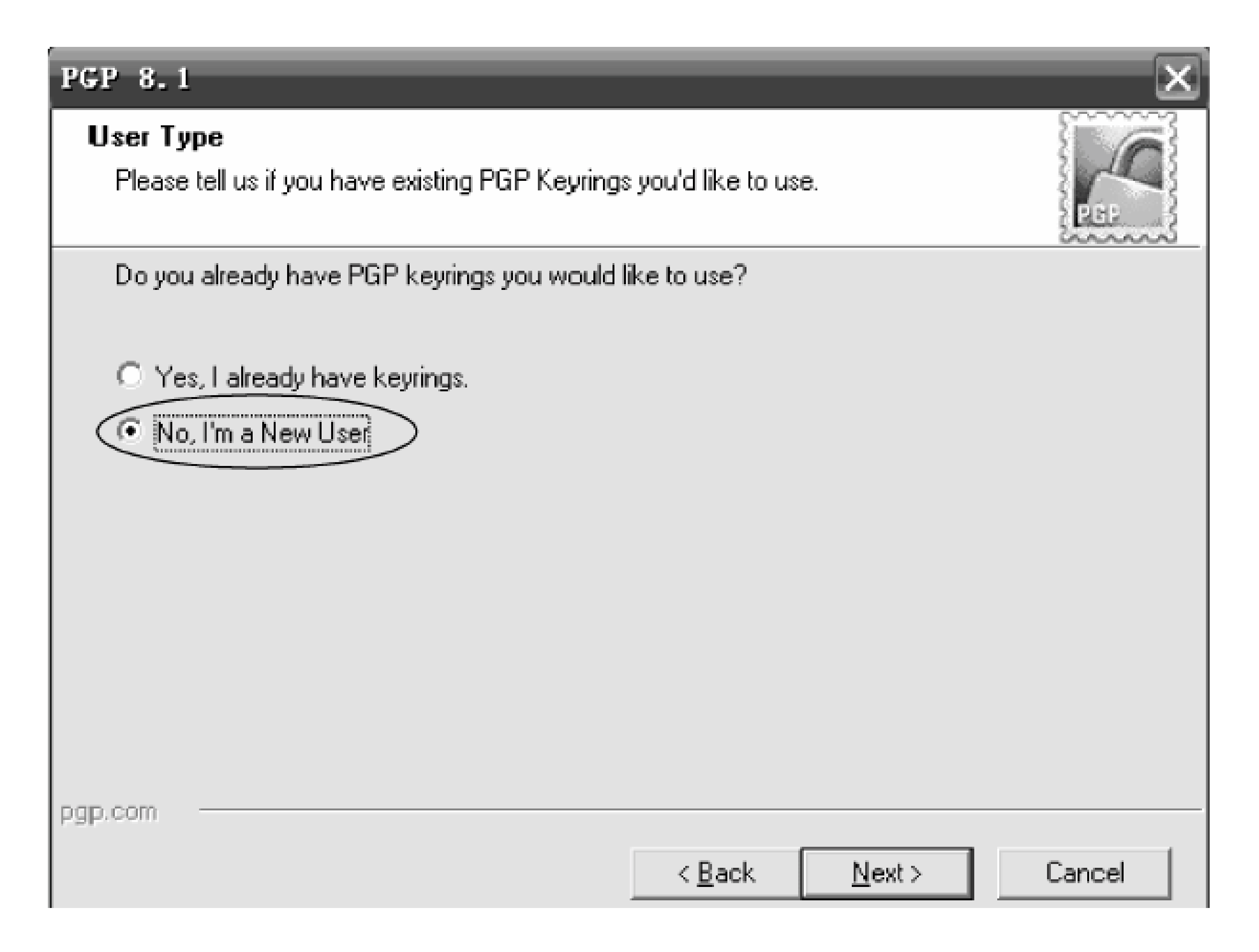


图 4.6　用户类型提示

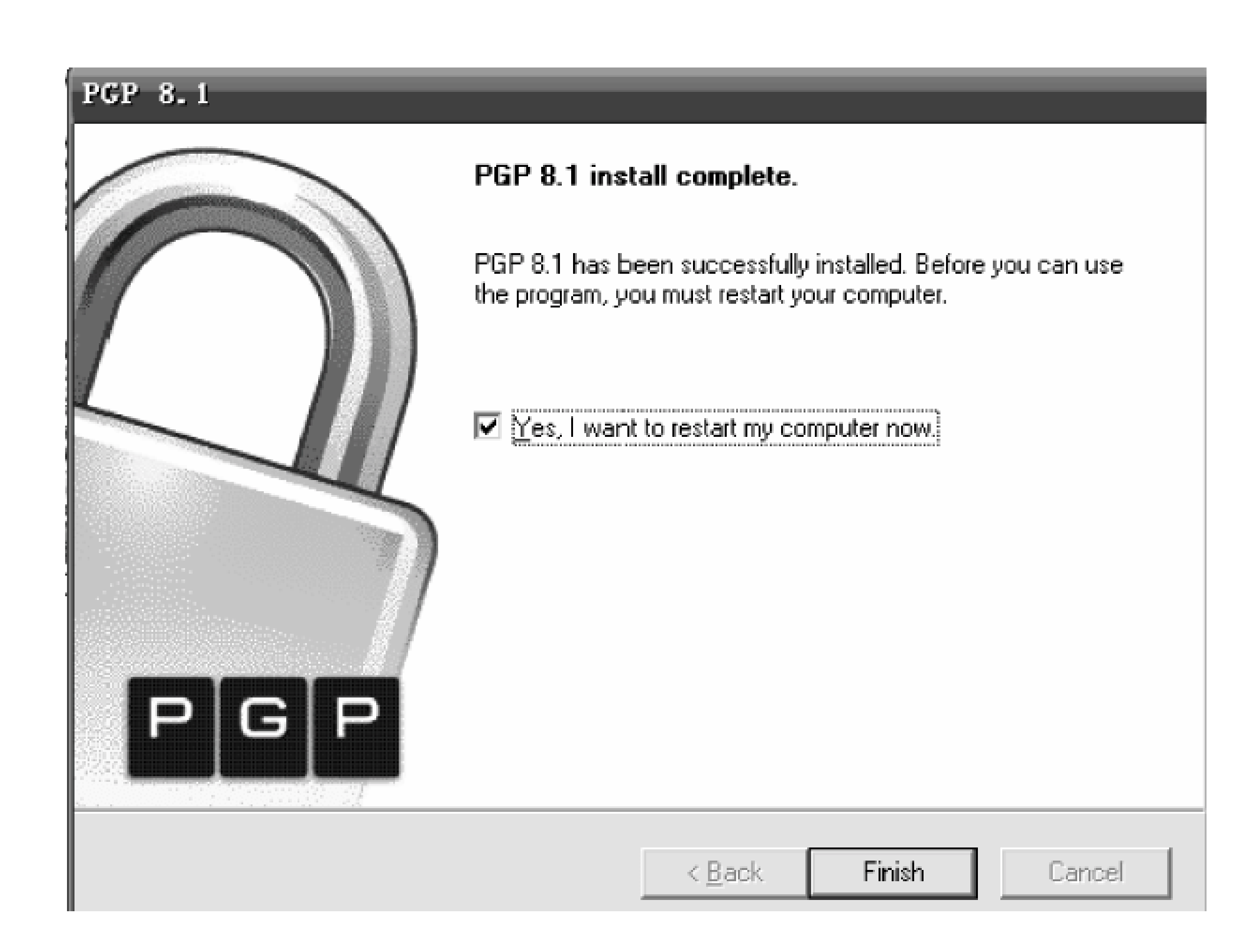


图 4.7　安装完毕要求重启机器

重启后进入密钥选取阶段。按提示给出用户全名和邮件地址后，选取密钥并再次确认该密钥，如图 4.8 所示，密钥选取后单击“下一步”按钮。这次选取的是对称密钥（即加密数据用的 IDEA 密钥）。

RSA 和 DH 都是公钥密码系统算法，它们的密钥都有两个，即公钥和私钥对。下面来选取公钥和私钥。

PGP 软件包中有 Documentation、PGPdisk、PGPkeys 和 PGPmail 四项。单击“开始”→“程序”→PGP 命令找到 PGP 软件包，从中选择 PGPkeys 选项，可看到如图 4.9 所示窗口。选择该窗口工具栏最左端的选择密钥对的工具项，可得到相应的 PGP 加密和签名用的公钥（pubring）与私钥（secring），如图 4.10 所示。选取公钥和私钥对后，用户要小心保存自己的私钥，把公钥通过你的朋友签名发送给其他朋友，或发到网上公共的 PGP 管理服务器。

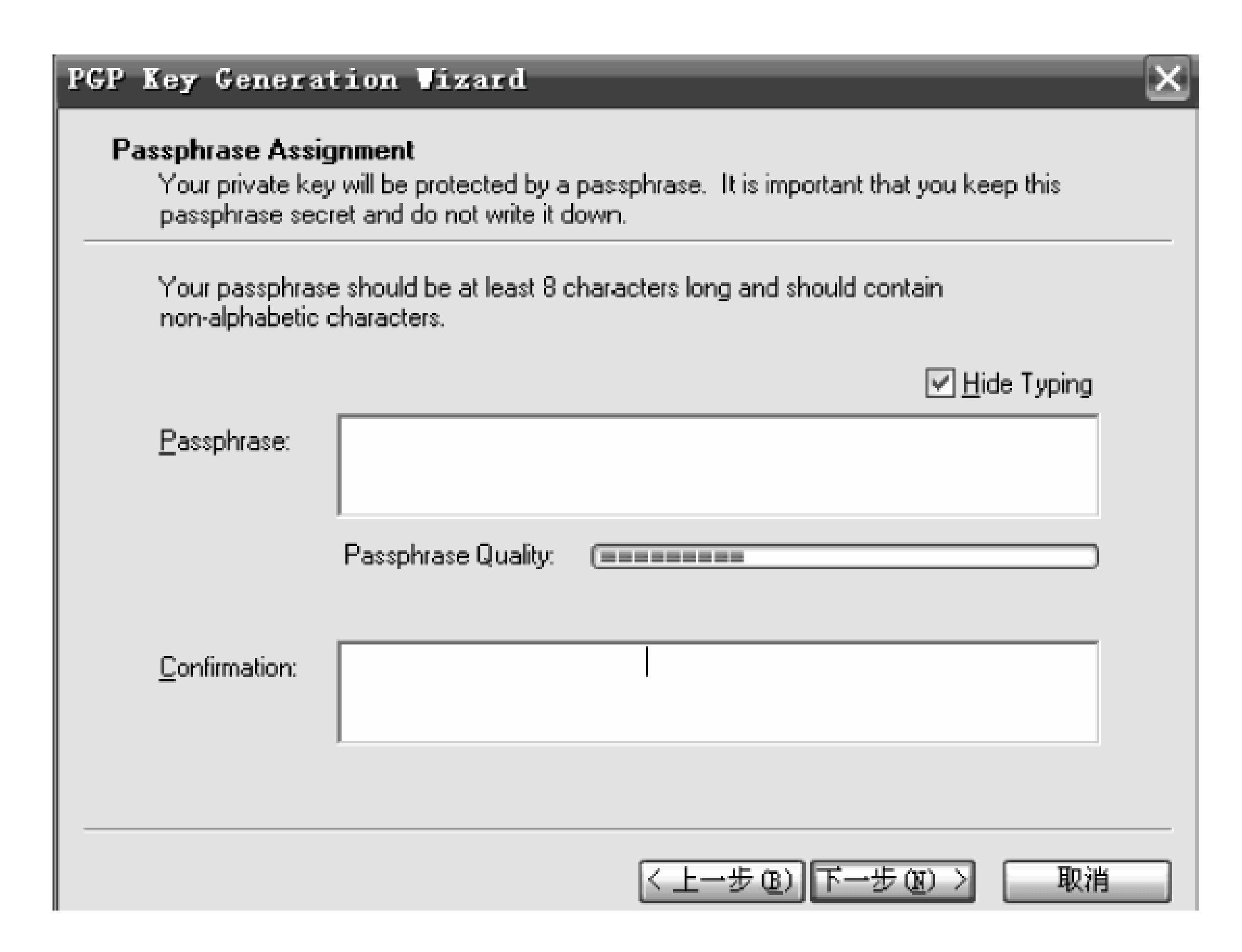


图 4.8　选取密钥并确认

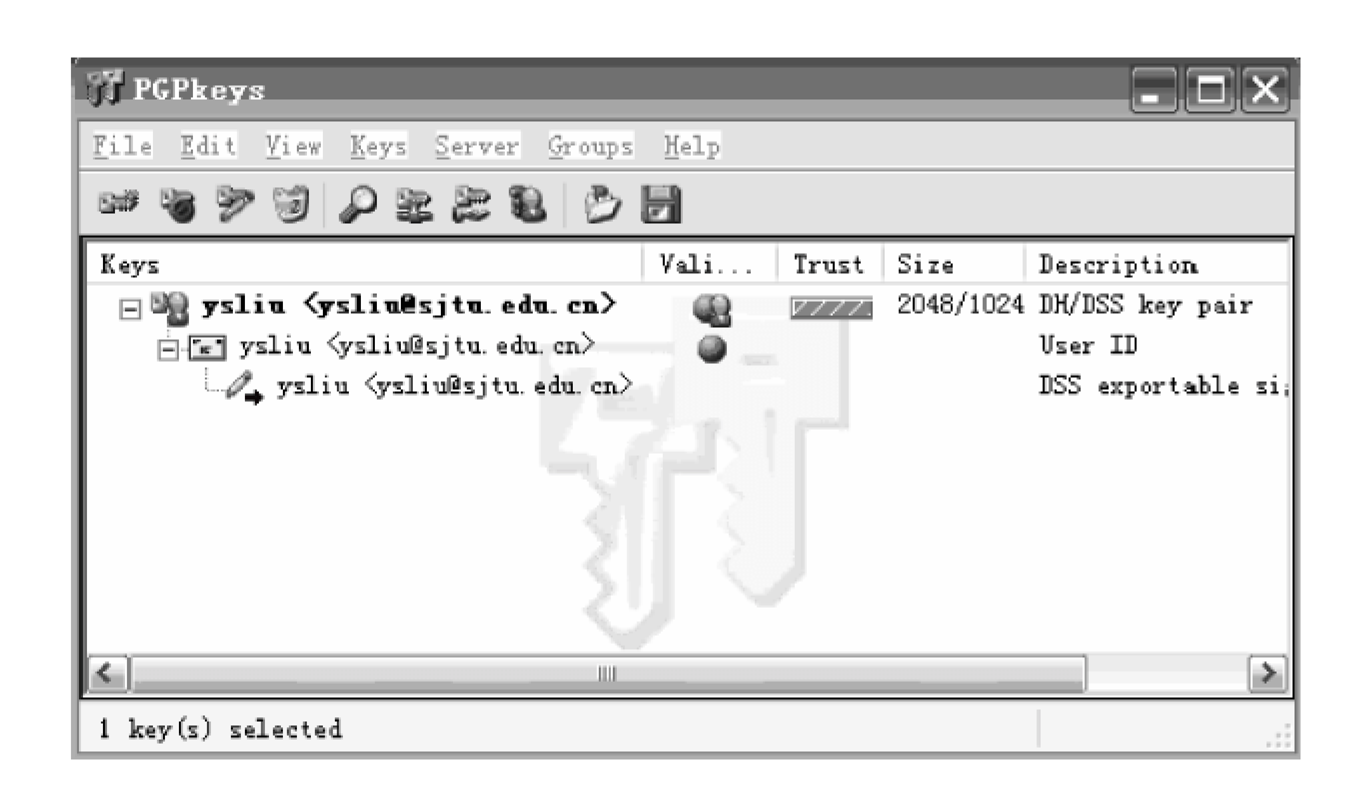


图 4.9　PGPkeys 窗口

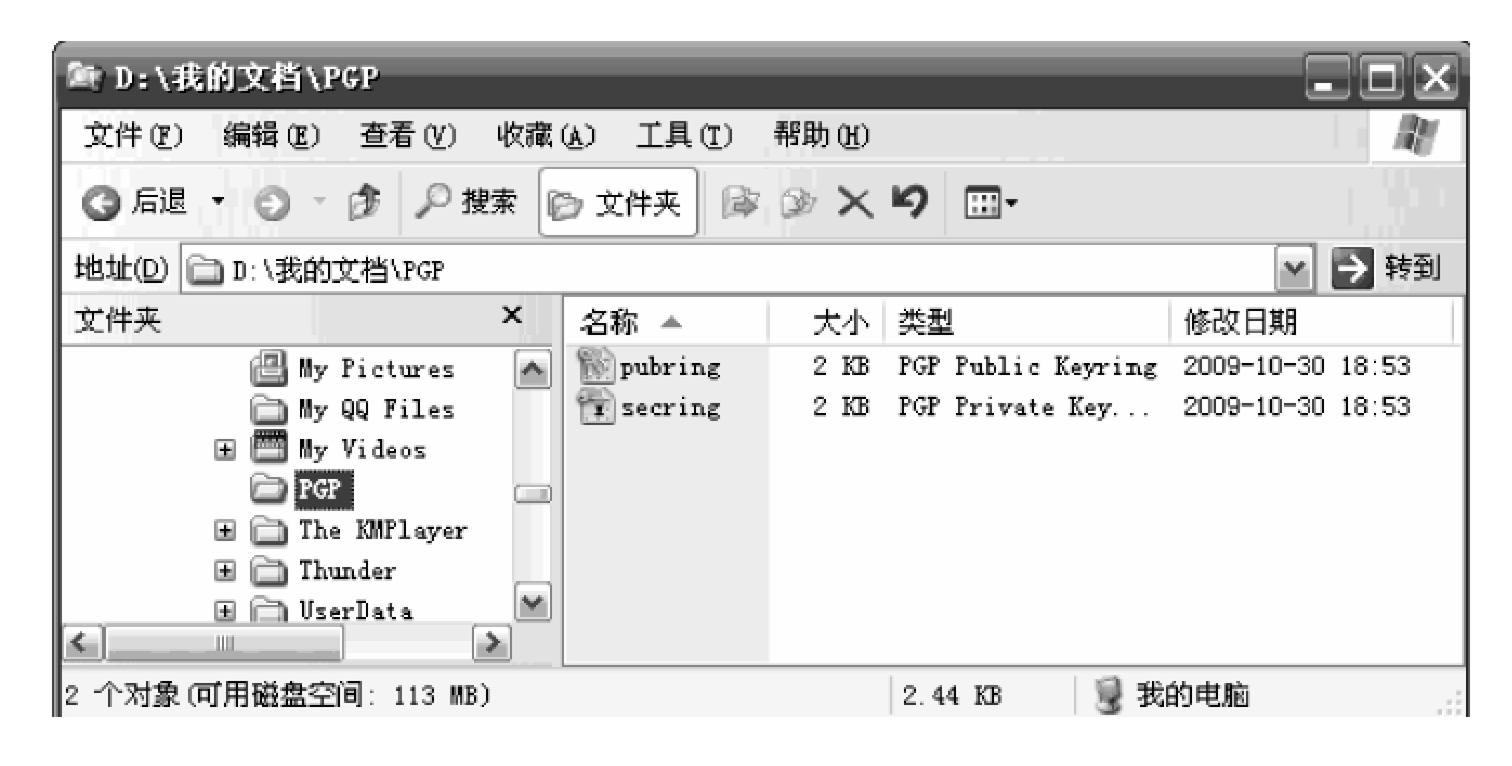


图 4.10　公钥和私钥显示

(3) 加密

单击“开始”→“程序”→PGP 命令找到 PGP 软件包，从中选择 PGPmail，可得到如图 4.11 所示的工具箱。该工具箱有 7 个按



图 4.11　工具箱

钮图标,从左到右依次为 PGPkeys(选密钥)、Encrypt(加密)、Sign(签名)、Encrypt & Sign(加密并签名)、Decrypt/Verify(解密并验证)、Wipe(文件销毁)和 Freespace Wipe(空间擦除)。

选择工具箱中的 Encrypt 可进行文件加密。首先在单击 Encrypt 工具后出现的对话框中选择要被加密的文件,如图 4.12 所示。单击"打开"按钮后弹出如图 4.13 所示对话框。在对话框中选择要加密文件的阅读者(中间栏带有邮件地址的部分可以是别人的,也可以是自己的)。该对话框中的选项 Text Output、Input Is Text、Wipe Original 和 Conventional Encryption 分别表示"输出文本形式的加密文件"、"输入的是文本文件"、"彻底销毁原始文件"和"用传统密码体制加密"(不用公钥系统,只能留着自己看)。选中 Text Output,单击 OK 按钮即可得到已加密的文件,密文并以文本形式存储,如图 4.14 所示。



图 4.12 选择加密的文件

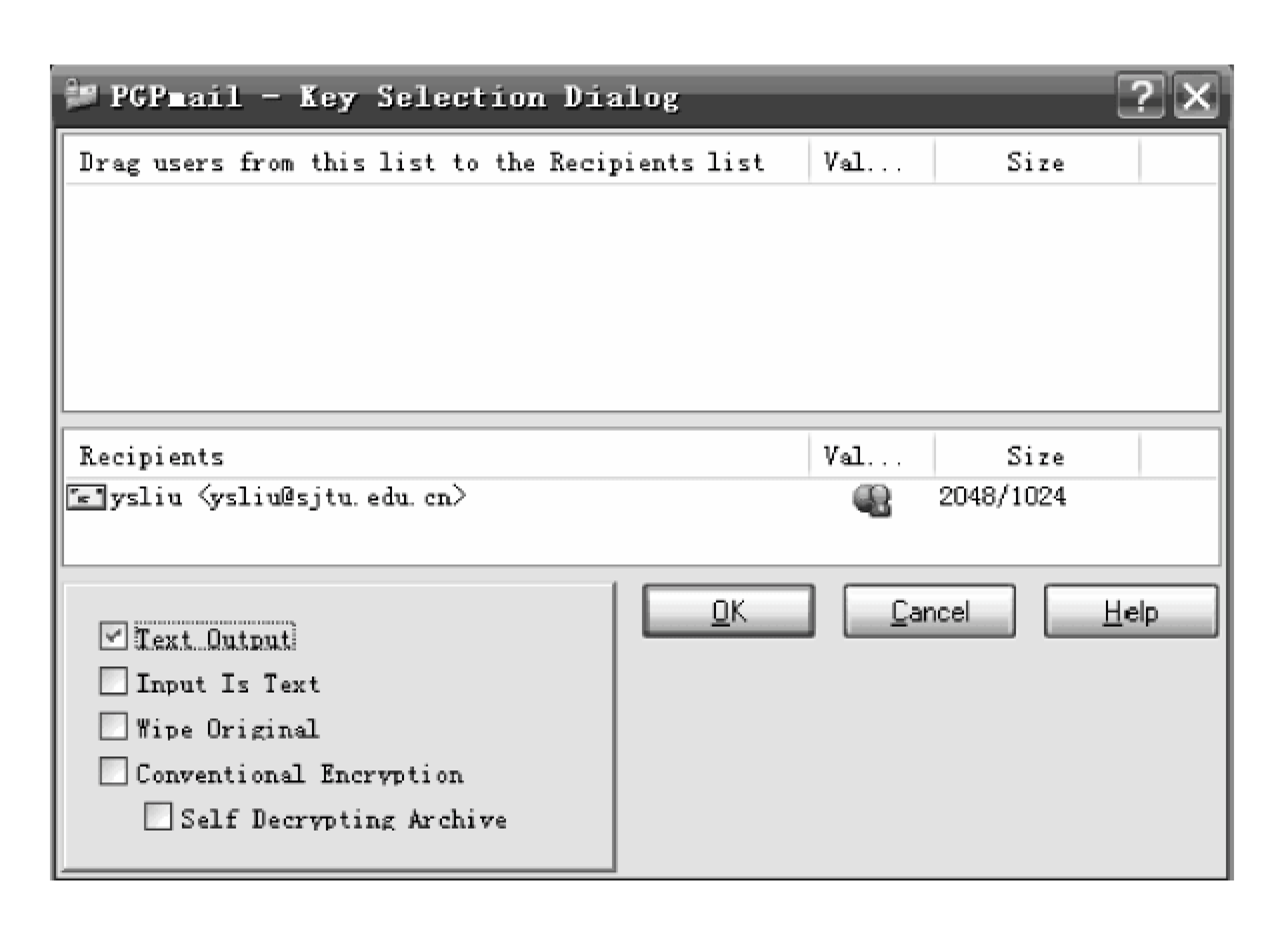


图 4.13 选择加密文件阅读者

(4) 签名

选择工具箱中的 Sign 可进行文件签名。首先在单击 Sign 工具后出现的对话框中选择要被签名的文件,如图 4.12 所示。然后单击"打开"按钮后弹出要求输入密码的窗口。输入密码后单击 OK 按钮,即可得到签过名的文件,签过名的文件被加上较形象的标记,如图 4.14 所示。签名后会出现一个记录窗口,该记录包括用户名、签名者、密钥 ID 号、有效(有法律效力)状态和日期。

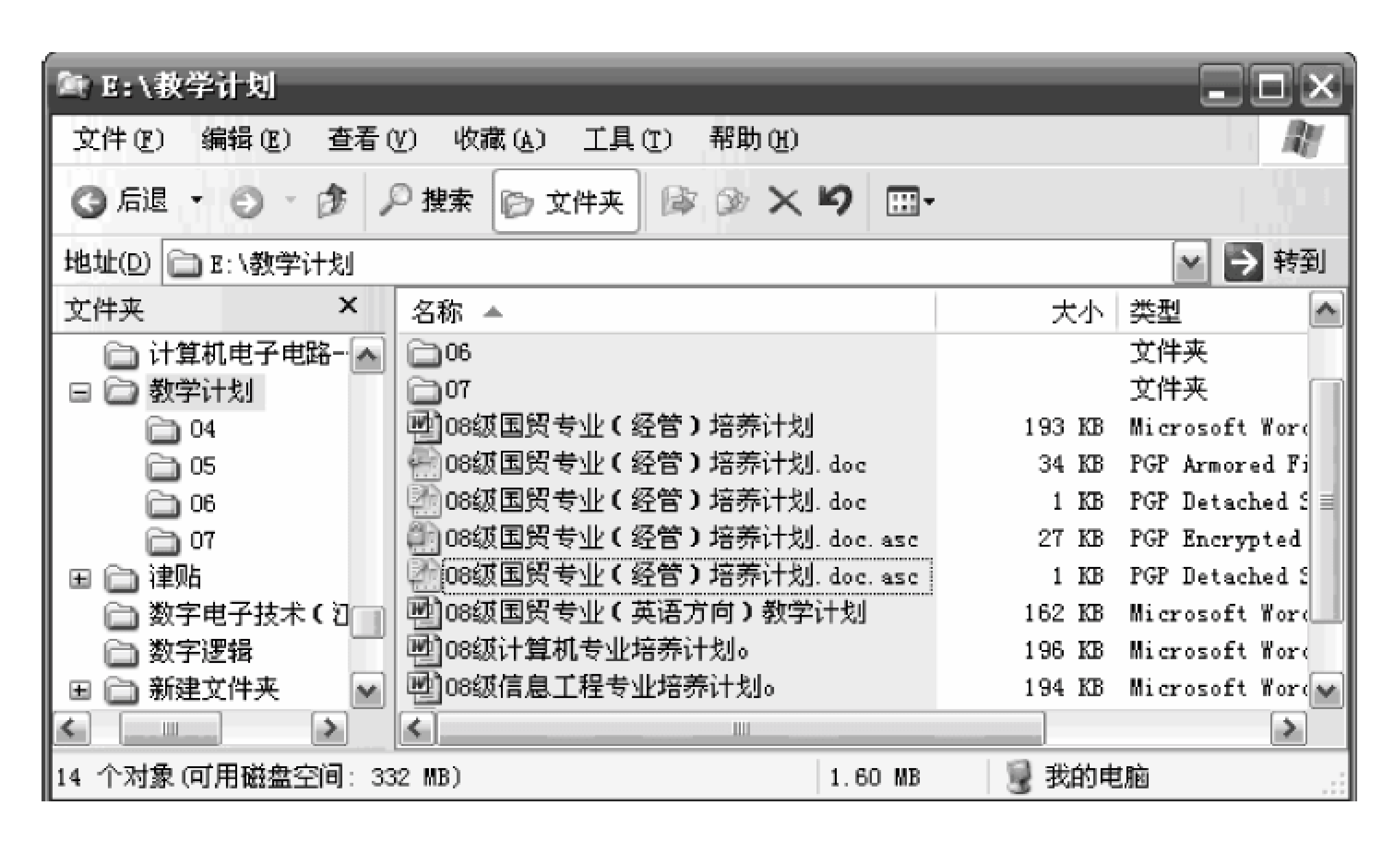


图 4.14　加密和签名的文件显示

此后的加密并签名、解密并验证、文件销毁和存储空间擦除等操作由读者自己完成。

4.4.2　CA 认证与数字证书应用

1. CA 认证与证书服务

在进入网络化时代后，许多部门也许会经常遇到这样的困惑：在内部进行网络管理时怎样在网上确认员工的身份，网上交易时对方发出的信息是否真实可信，网上纳税时怎样有效地表明企业的身份等。由此可见，“信任”是每个网上交易（交换）实体（网络用户）进行各种网上行为的基础。构架一个安全可信的网络环境是各种网上操作顺利开展的有力保障。在常规的交易业务中，交易双方现场交易，可以很容易确认买卖双方的身份。但在网上进行的电子商务交易，交易双方并不在现场，买方和卖方都希望在 Internet 上进行的一切交易运作都是真实可靠的。保证交易双方身份的真实性和交易的不可抵赖性，已经成为人们迫切关心的问题。因此，必须保证网上的交易过程是十分可靠的，保证交易中能够实现身份认证、安全传输、不可否认和数据一致性。CA 认证就是网络的一种安全控制技术，它可以提供网上交易所需的“信任”。CA 认证的出现和数字证书的使用，使得开放的网络更加安全。

（1）CA 认证中心

① CA 认证

CA 的英文全称是 Certificate Authority，即证书授权中心，也叫认证中心。在网上电子交易中，商户需要确认持卡人是否是信用卡或借记卡的合法持有者，同时持卡人也要能够鉴别商户是否合法商户，是否被授权接受某种品牌的信用卡或借记卡。为处理这些问题，必须有一个大家都信赖的机构来发放一种证书。这种证书就是数字证书，它是参与网上交易活动的各方（如持卡人、商家、支付网关）身份的证明。每次交易时，都要通过数字证书对各方的身份进行验证。CA 认证中心作为权威的、可信赖的、公正的第三方，是发放、管理、废除数字证书的机构。

② X.509 标准

X.509 是国际电信联盟（ITU-T）建议作为 X.500 目录检索的一部分，提供安全目录检

索服务，是一种行业标准或行业解决方案。在 X.509 方案中，默认的加密体制是公钥密码体制。为进行身份认证，X.509 标准及公钥密码系统提供了数字签名方案。用户可生成一段信息及其摘要（信息“指纹”），再用专用密钥对摘要加密以形成签名，接收者用发送者的公钥对签名解密，并将其与收到的信息“指纹”进行比较，以确定其真实性。

此问题的解决方案即 X.509 标准与公钥证书。本质上，数字证书由公钥和密钥拥有者的用户标识组成，整个字块由可信赖的第三方签名。

CA 认证中心颁发的数字证书均遵循 X.509 v3 标准。基于 X.509 证书的认证技术适用于开放式网络环境下的身份认证。该技术已被广泛接受，许多网络安全程序都可以使用 X.509 证书。X.509 是一种非常通用的证书格式。所有的证书都符合 ITU-T X.509 国际标准，因此，为一种应用创建的证书可以用于任何其他符合 X.509 标准的应用。在一份证书中，必须证明公钥及其所有者的姓名是一致的。对 X.509 证书来说，认证者总是 CA 或由 CA 指定的人。一份 X.509 证书是一些标准字段的集合，这些字段包含有关用户或设备及其相应公钥的信息。X.509 证书包含的内容有 X.509 版本号、证书持有人的公钥、证书的序列号、主题信息、证书的有效期、认证机构（证书发布者）、发布者的数字签名和签名算法标识符。

③ CA 的功能

CA 认证中心所发放的数字证书就是网络中标志通信各方身份信息的电子文件，它提供了一种在 Internet 上验证用户身份的方式。数字证书的作用类似于司机的驾驶执照或日常生活中的身份证。人们可以在交往（交易）中使用数字证书来识别对方的身份。

CA 认证中心就是一个负责发放和管理数字证书的权威机构。CA 的作用是检查证书持有者身份的合法性，并签发证书（在证书上签字），以防证书被伪造或篡改，以及对证书和密钥进行管理。如果说数字证书就相当于用户在网上的个人电子身份证，同日常生活中使用的个人身份证一样，则 CA 就相当于网上公安局，专门发放、管理和验证身份证。

CA 认证中心的主要功能有颁发证书、更新证书、查询证书、废除证书和证书归档等。

（2）数字证书

数字证书是一个经 CA 认证中心数字签名的、包含公钥拥有者信息和公钥的文件。最简单的证书包含一个公钥、名称以及 CA 中心的数字签名。一般情况下证书中还包括密钥的有效时间、发证机关的名称和该证书的序列号等信息。

① 数字证书的功能

数字证书认证是基于国际 PKI（公开密钥基础设施）标准的网上身份认证系统进行的。数字证书以数字签名的方式通过第三方权威认证有效地进行网上身份认证，帮助网上各个交易实体识别对方身份和表明自己的身份，具有真实性和防抵赖功能。与物理身份证不同的是，数字证书还具有安全、保密、防篡改的特性，可对网上传输的信息进行有效的保护和安全传输。例如，随着电子政务的发展，网上报税必将成为许多企业进行日常税务申报的常用方式。网上报税即由税务部门建立专门的申报网站，纳税户通过 Internet 访问税务部门网站上的网上报税系统，正确填写电子化申报表后，传送申报数据至税务部门服务器，税务部门对这些数据进行处理、储存，并将处理结果反馈给纳税人。在此过程中，纳税人通过使用标识其身份的数字证书登录网上纳税服务系统，就可以安全地进行网上税务申报。所有诸如企业账号、纳税额等申报信息都经过高强度加密，保证信息可以安全无误地在纳税人与税

务系统中传输,同时也可以表明该企业的有效身份并证明其纳税实事。即使有人从中非法截获有关信息,他也无法知道真实内容。

以加密技术为核心的数字证书可以对网络上传输的信息进行加密和解密、签名和验证,确保网上传递信息的保密性、完整性,以及交易实体身份的真实性和签名信息的不可否认性,从而保障网络应用的安全性。数字证书主要有以下 4 大功能。

- 保证信息的保密性。交易中的商务信息均有保密的要求,如信用卡的账号和用户名被人知悉,就可能被盗用;订货和付款的信息被竞争对手获悉,就可能丧失商机。而数字证书可保证电子商务中传输信息的保密性。
- 保证信息的完整性。交易中数据文件要保持其完整性,不可被修改和增删。数字证书可确保电子交易文件的完整性,以保证交易的严肃性和公正性。
- 保证交易者身份的真实性。网上交易的双方大多素昧平生,相隔千里。要使交易成功首先要能确认对方的身份。对于为客户服务的银行、信用卡公司和销售商家,为了做到安全、保密、可靠地开展服务活动,都要进行身份认证的工作。数字证书可保证网上交易双方身份的真实性,银行和信用卡公司可以通过 CA 认证确认身份,放心地开展网上业务。
- 保证交易的不可否认性。由于商情的千变万化,交易一旦达成是不可否认的,否则必然会损害交易中一方的利益。数字证书具有可防止这种否认(抵赖)性的功能。

② 数字证书的应用

数字证书利用一对互相匹配的密钥进行加密和解密。每个用户自己设定一个特定的仅为本人所知的私钥,用它进行解密和签名;同时设定一个公钥并公开,以便为公众所共享,用于加密和验证签名。当发送一份保密文件时,发送方使用接收方的公钥对数据加密,而接收方则使用自己的私钥解密,这样信息就只有合法接收方能够解密。通过数字的手段保证加密过程是一个不可逆过程,即只有用私钥才能解密。

数字证书可应用于网上的行政管理和商务活动,如用于发送安全电子邮件、访问安全站点、网上证券、网上银行、网上招投标、网上签约、网上办公、网上缴费、网上纳税等网上安全电子事务处理和安全电子交易活动。其应用范围涉及需要身份认证及数据安全的各个行业,包括传统的商业、制造业、流通业的网上交易,以及公共事业、金融服务业、工商、税务、海关、教育科研单位、保险、医疗等网上作业系统。

2. 数字证书应用实例

目前,数字证书被广泛应用于网上银行、网上交易等商务活动中。使用数字证书还可以对数据和电子邮件进行加密和签名。下面介绍数字证书申请和几个数字证书的应用实例,读者从中可以更好地了解数字证书的应用。

(1) 数字证书的申请

在 Outlook Express 中可以通过数字签名来证明邮件发送者的身份,即让对方确信该邮件是由你的机器发送的。Outlook Express 同时提供邮件加密功能,可使邮件只有合法接收者才能接收并阅读,但前提是必须先获得对方的数字标识(数字证书)。

要对邮件进行数字签名必须首先获得一个私人的数字标识(digital ID),即用户的数字证书。数字标识是指由独立的授权机构发放的证明你在 Internet 上身份的证件。用户应先

向这些公司申请数字标识,然后就可以利用这个数字标识对你写的邮件进行数字签名。如果获得了别人的数字标识,还可以给别人发送加密邮件。

目前 Internet 上有较多商业性的数字证书发证机构,其中 VeriSign 公司是 Microsoft 的首选数字证书提供商。通过 VeriSign 的特别馈赠,IE 用户可获得一个免费使用 60 天的数字标识。

下面就以该公司为例介绍数字证书的申请方法:直接进入 VeriSign 公司的申请页面 http://www.verisign.com/client/index.html,单击中间黄底上的 BUYNOW 按钮,如图 4.15 所示;在下一页面选择 Microsoft Internet Explorer,如图 4.16 所示。在接下来的页面中要求先填一张表,如图 4.17 所示,按提示填入个人信息及电子邮件地址。填表时有一项为 Challenge Phrase,直译为"盘问短语",是当想取消数字标识时 VeriSign 公司确认是否是合法拥有者的询问口令。如果不能正确答出这个短语,数字标识将一直使用到期满为止。还有一项 Payment Information 是针对收费用户的,如果在前面选的是 I'd like to test drive a 60-day trial Digital ID for free 即先试用 60 天,则此项不填。确认无误并提交后,过一会儿(大约十分钟之内)你就会收到一封 VeriSign 公司发来的电子邮件,其中就包含数字标识 PIN。

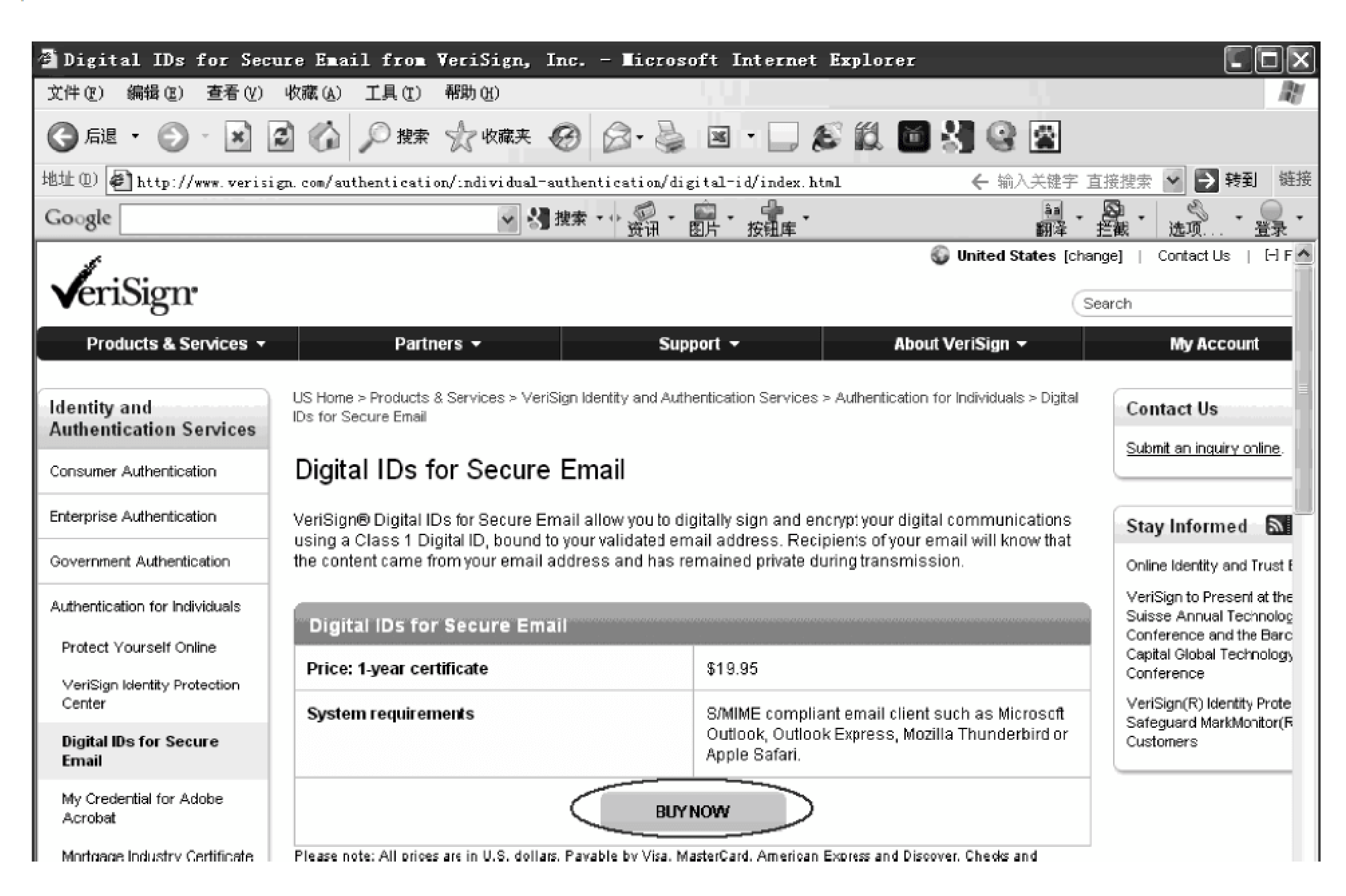


图 4.15 VeriSign 的证书申请窗口

一般情况下只需简单地单击最后那个 NEXT 按钮就可以继续了,不过有时可能会提示上一页面错误,建议直接将回信中提供的 PIN 复制下来,然后将其填到 https://digitalid.verisign.com/enrollment/mspickup.htm 页面下输入 PIN 的对话框内,如图 4.18 所示,单击 Submit(提交)按钮;在弹出的如图 4.19 所示窗口中单击 INSTALL(安装)按钮,开始安装数字标识到本机的 Outlook Express 中。至此,数字证书的申请完成。



图 4.16 选择证书提供商

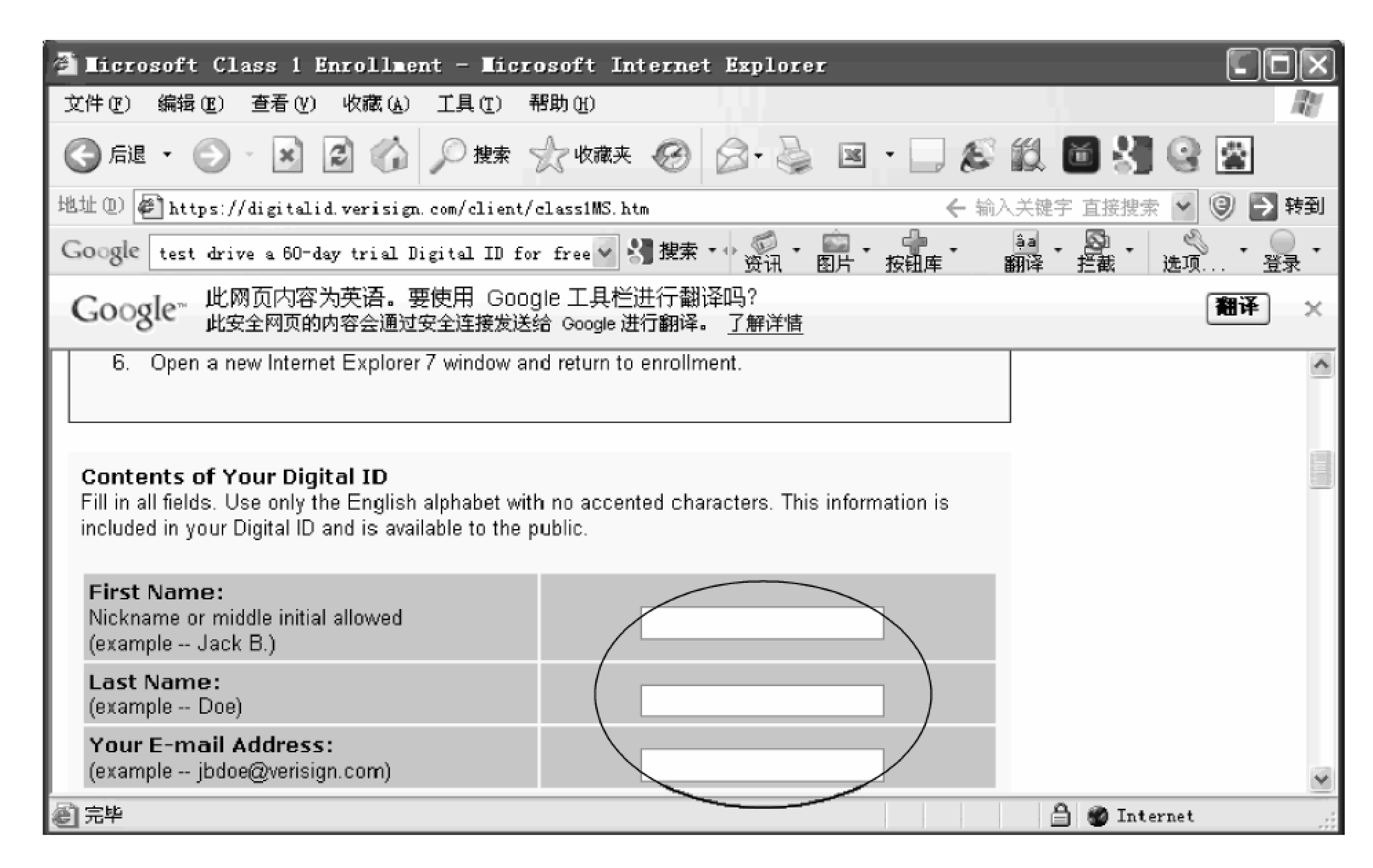


图 4.17 填写个人信息

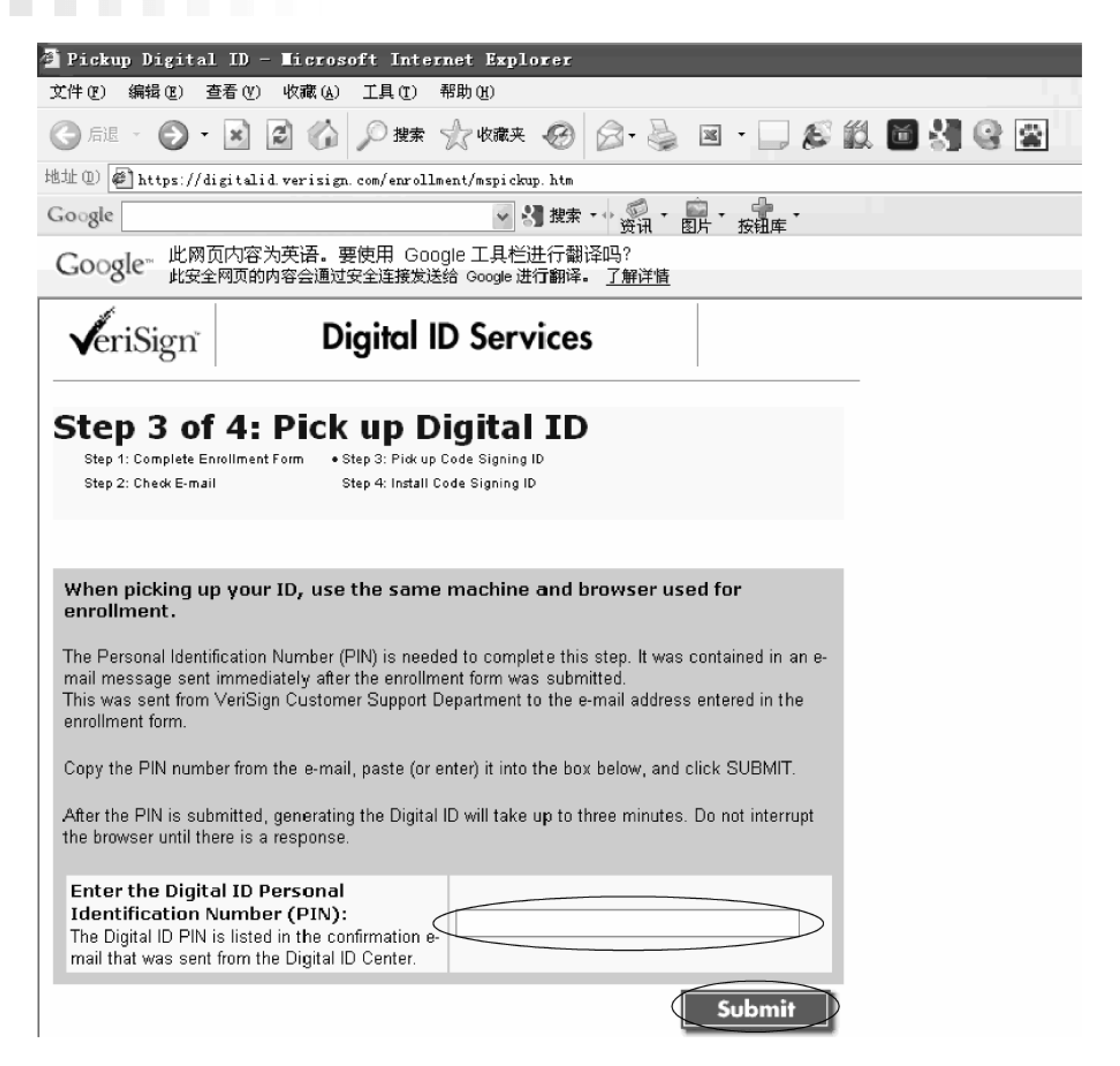


图 4.18 填写 PIN





图 4.19 安装证书到本机

安装过程中可能出现如图 4.20 所示的“潜在的脚本冲突”情况，单击“是”按钮即可。

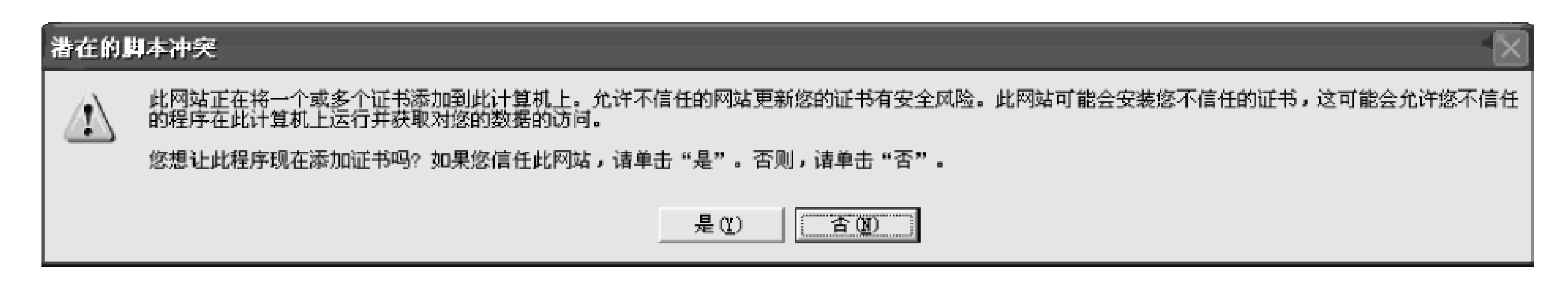


图 4.20　潜在的脚本冲突

用户得到的数字证书的常规信息如图 4.21 所示，其详细信息包括版本、序号、签名算法、颁发者、有效起始日期、有效截止日期、公钥、基本限制、密钥用法等；证书路径如图 4.22 所示。

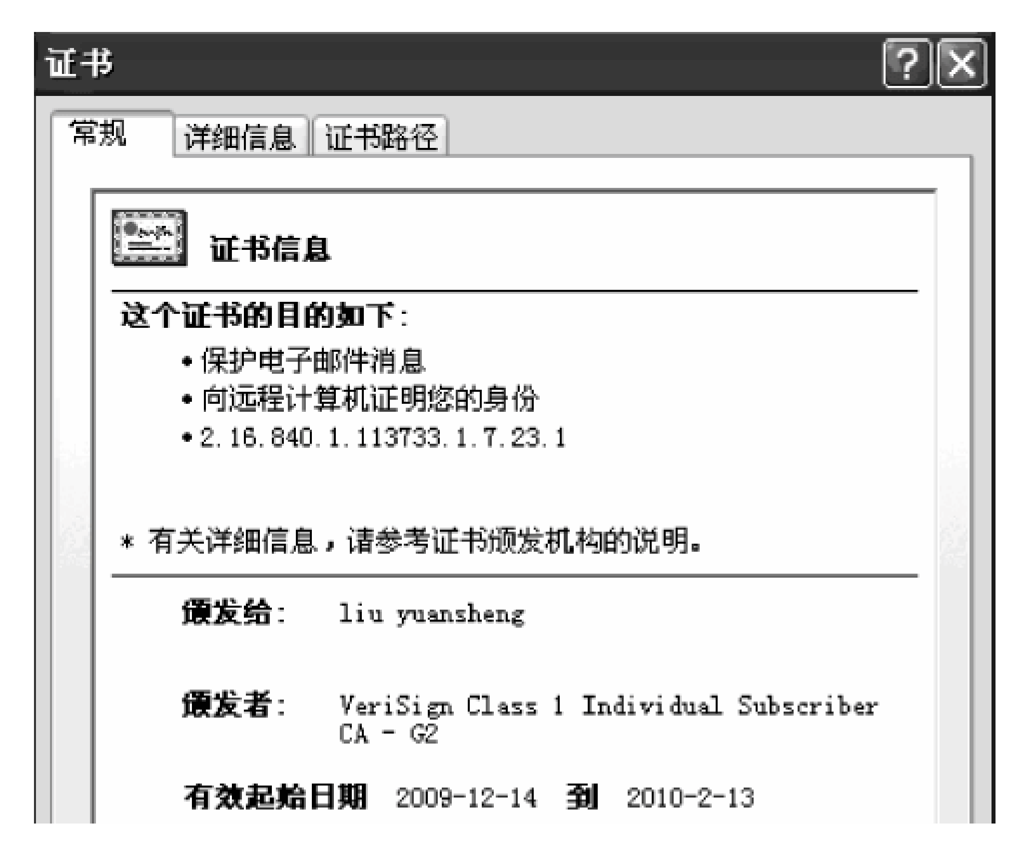


图 4.21　数字证书信息

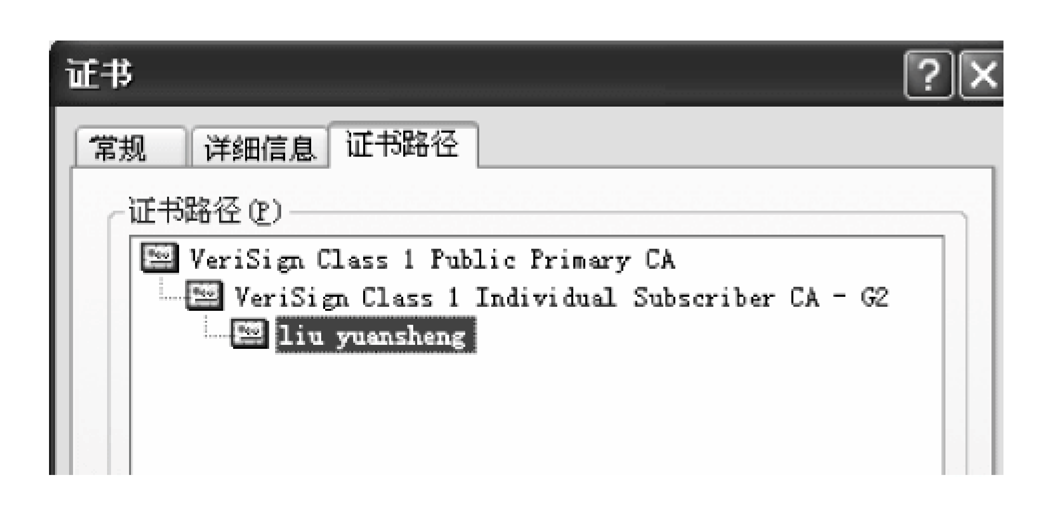


图 4.22　数字证书路径

(2) 利用数字证书签名和加密电子邮件

获得数字证书后，就可以利用它对电子邮件进行签名和加密，这样可保证发送的邮件不会被篡改，外人又无法阅读加密邮件的内容。现在以 Outlook Express 为例，介绍利用数字证书对电子邮件进行签名和加密的方法。

启动 Outlook Express，在主窗口单击“工具”→“选项”菜单，选择“安全”选项卡，弹出如图 4.23 所示页面。单击“高级”按钮，弹出如图 4.24 所示“高级安全设置”对话框，按图示勾选相应的安全设置，单击“确定”按钮退出。

发送数字签名邮件时，可使用数字标识(证书)进行签名。如果希望对所有待发的邮件都进行数字签名，可在如图 4.23 所示的“安全”选项卡下勾选“在所有待发邮件中添加数字签名”复选框；如果只希望对某一封邮件进行数字签名，则不要选择该复选框，只需在每次撰写邮件后按下工具栏右上端的“签名”按钮即可。在图 4.23 中，单击“数字标识”按钮，在出现的“证书”对话框选择要使用的证书，如图 4.25 所示。

图 4.25 中的“导入”是帮助用户将证书、证书信任列表和证书吊销列表从磁盘复制到证书存储区；“导出”是帮助用户从证书存储区将证书、证书信任列表和证书吊销列表复制到磁盘。如果要进行导入操作，单击“导入”按钮，弹出如图 4.26 所示的“证书导入向导”对话框，在文件名框中输入系统中已存在的证书文件(如“abcde”)，单击“下一步”按钮。

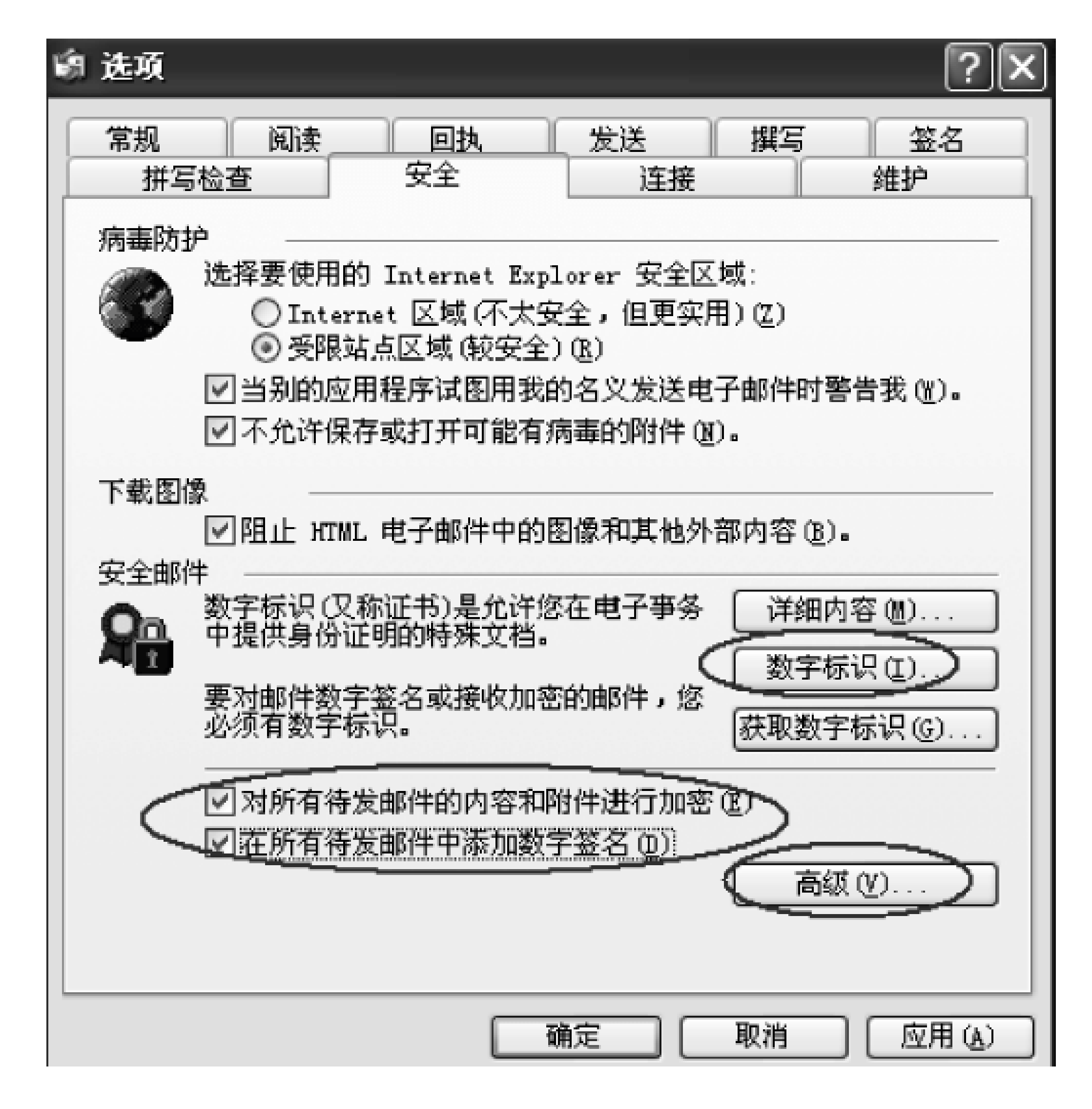


图 4.23　Outlook Express 安全选项



图 4.24　邮件高级安全设置



图 4.25　选择数字证书

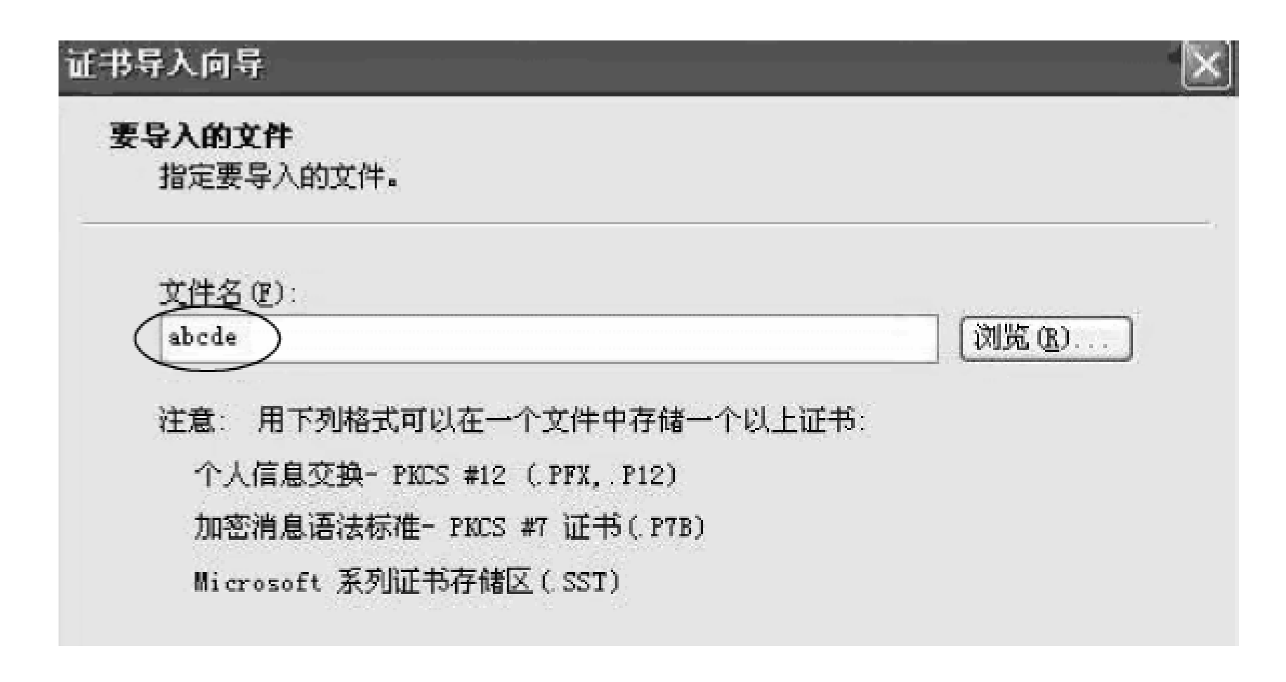


图 4.26　输入导入文件

进入 Outlook Express，选择“文件”→“新建”→“邮件”菜单，进入写邮件窗口，撰写新邮件。在填写好收件人地址和主题等相关信息并写好邮件后，单击页面右上方的“签名”工具，如图 4.27 所示。这就为要发邮件进行了签名，在右侧可见一个飘带状的数字签名标识，打开“工具”栏时也可看到“数字签名”前被打勾。这样，发出的这封邮件就是带有数字签名的邮件。

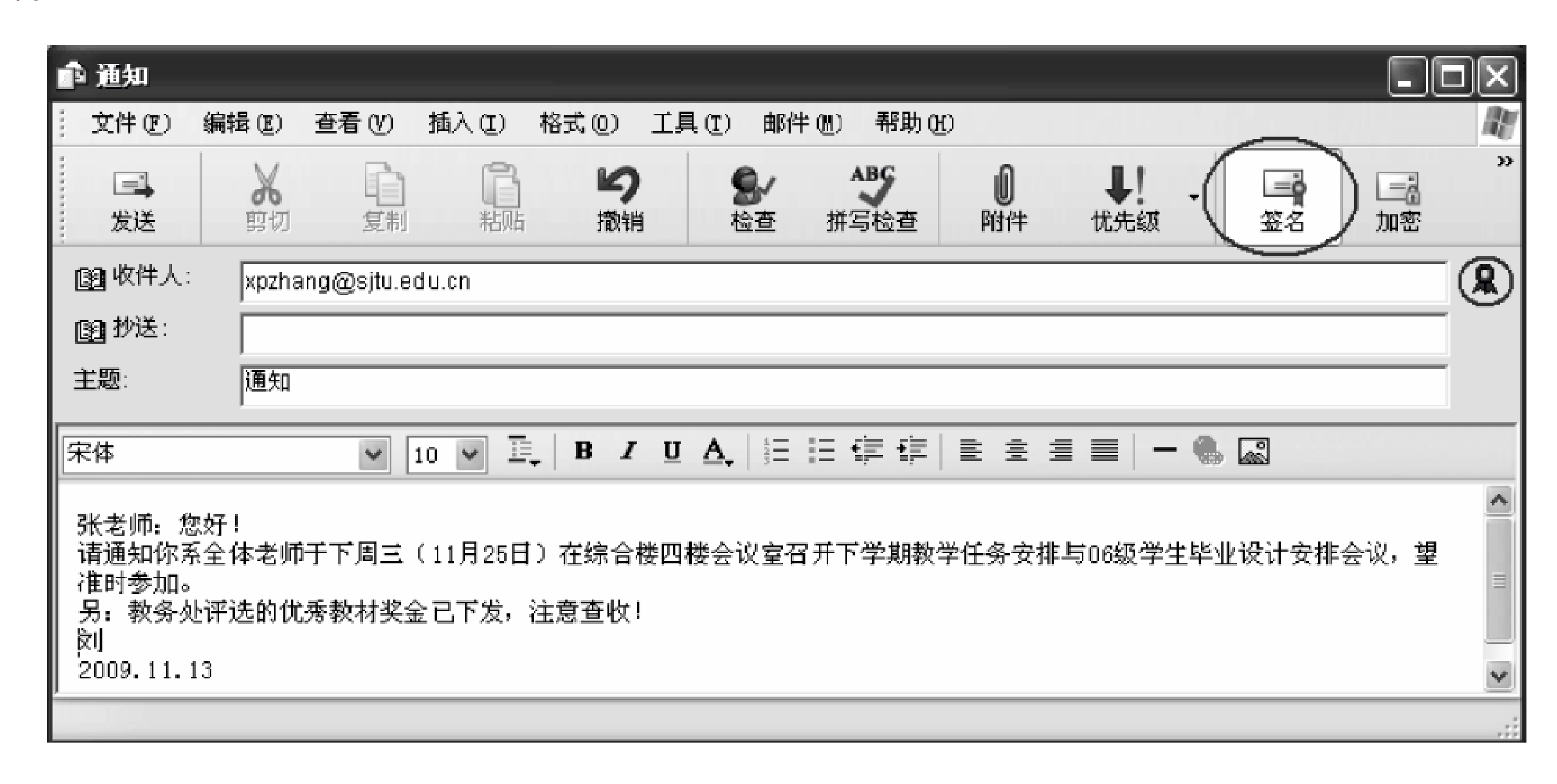


图 4.27　添加邮件数字签名

当收信方打开收到的签名邮件后，在附件中可见到如图 4.28 所示的证书文件夹，选择一个证书并双击证书后出现如图 4.29 所示证书页面，这就是发送方签名的数字证书(参见图 4.21)。邮件接收用户单击图 4.29 中的“安装证书”，出现证书导入的欢迎界面，单击“下一步”按钮，弹出如图 4.30 所示的“证书导入向导”对话框，选择证书存储区域后，再单击“下一步”按钮，证书导入成功。

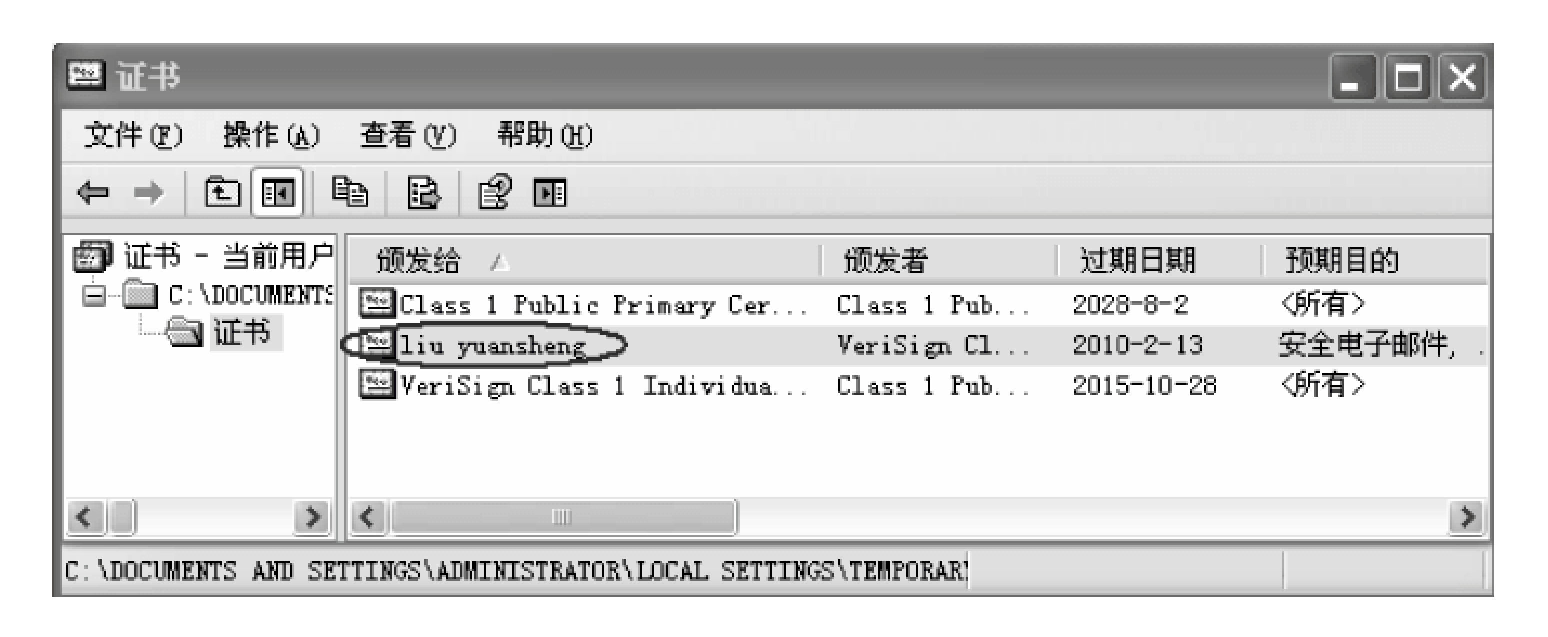


图 4.28　证书文件信息

发送加密邮件的方法与上述发送签名邮件的方法类似。如果希望对所有待发的邮件都进行加密，可在图 4.23 所示的“安全”选项卡下勾选“在所有待发邮件中添加数字签名”复选框；如果只希望对某一封邮件进行加密，只需在撰写邮件后单击工具栏右上端的“加密”按钮。当再次打开“工具”栏时即可看到 “加密”前被打勾，且在右侧可看到一个加密标识(一把小锁)，如图 4.31 所示。这样，发出的这封邮件就是加过密的邮件。

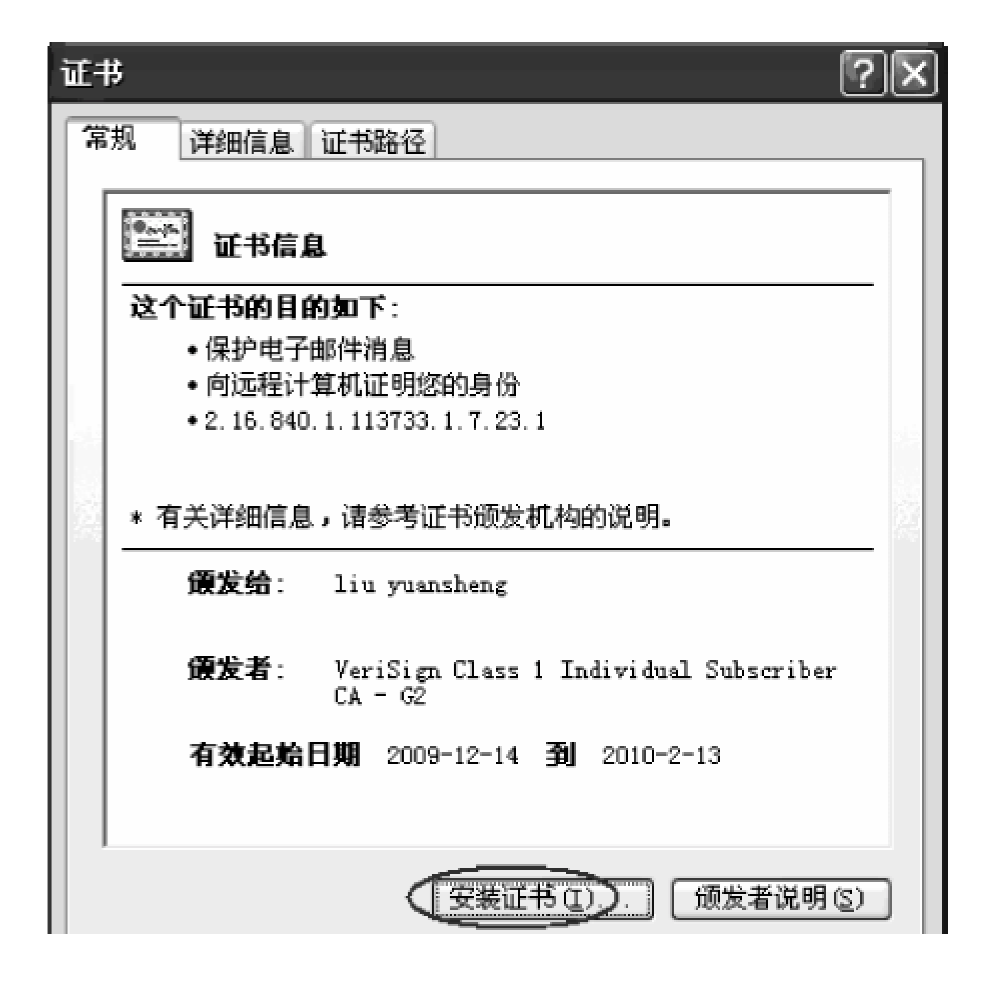


图 4.29 发送方的数字证书信息



图 4.30 证书存储区选择

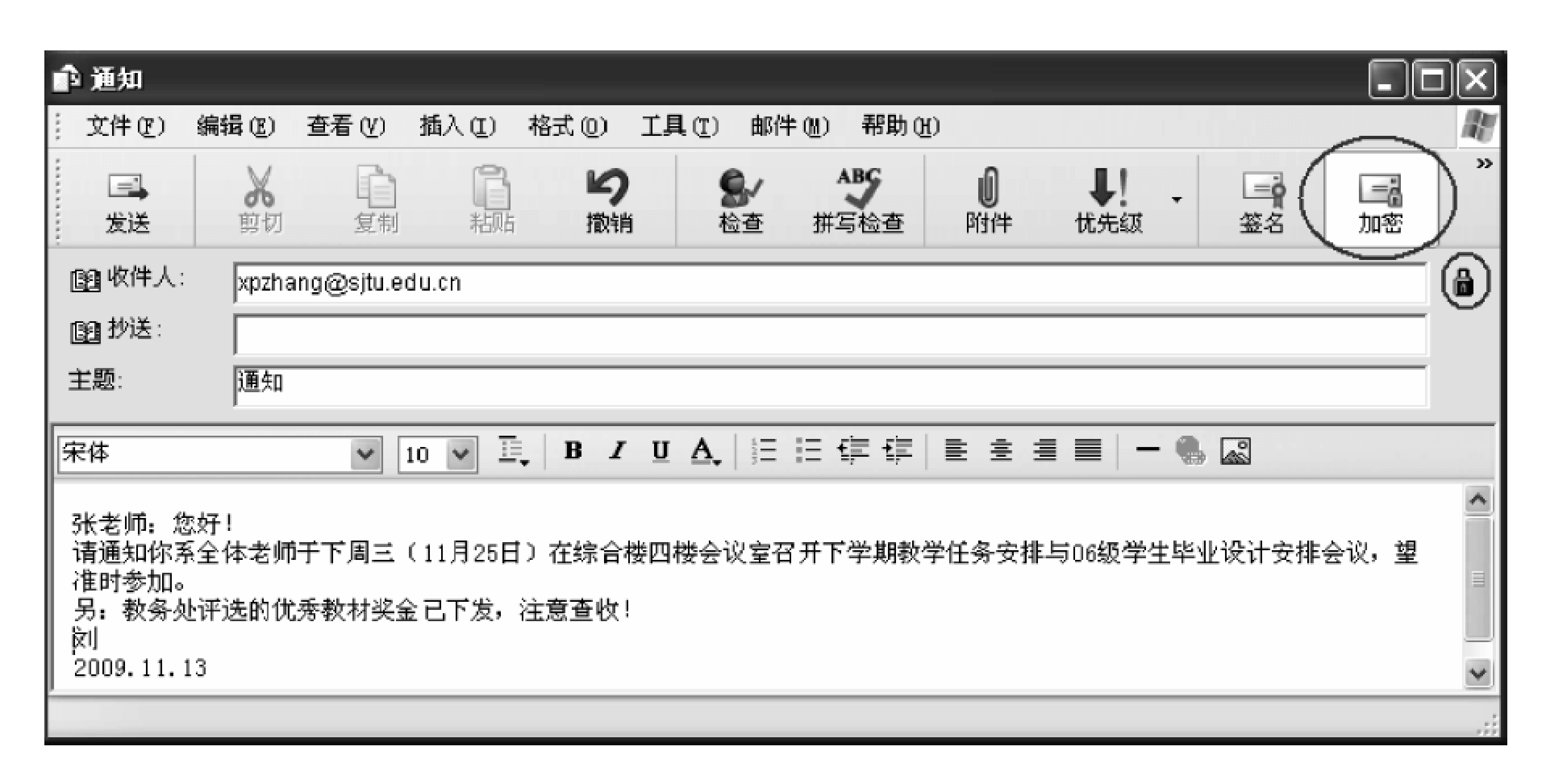


图 4.31 添加邮件加密

(3) 用数字证书对文档签名

打开要签名的 Word 文档(Office 2003/XP)，选择"工具"→"选项"菜单，单击"安全性"选项卡，如图 4.32 所示。单击中部左侧的"数字签名"按钮，随后会弹出一个如图 4.33 所示的"数字签名"对话框；单击"添加"按钮，从数字证书中选择一个(如"liu yuansheng")进行添加，如图 4.34 所示；然后单击"确定"按钮返回，得到添加的数字证书，如图 4.35 所示。现在数字证书就加到该文档中了，即该文档被加上数字签名。当再次打开签名后的该文件时，就会看到 Word 页面最上方显示的文件名后面的括号中有"已签名，未验证"字样。签名后的

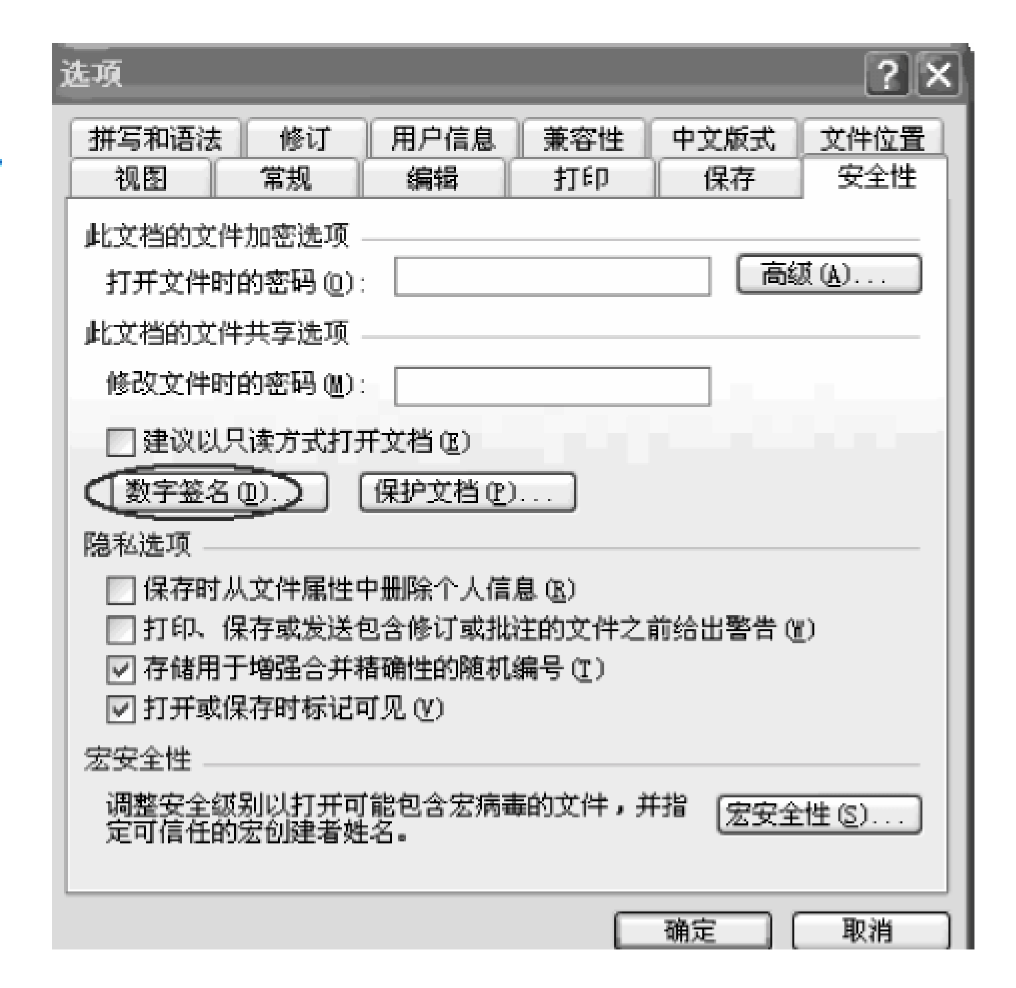


图 4.32 文档的安全性选项

文档不能再修改，若要保存修改的内容，则会取消其签名，如图 4.36 所示。



图 4.33　添加数字签名证书



图 4.34　选择数字签名证书



图 4.35　添加数字证书

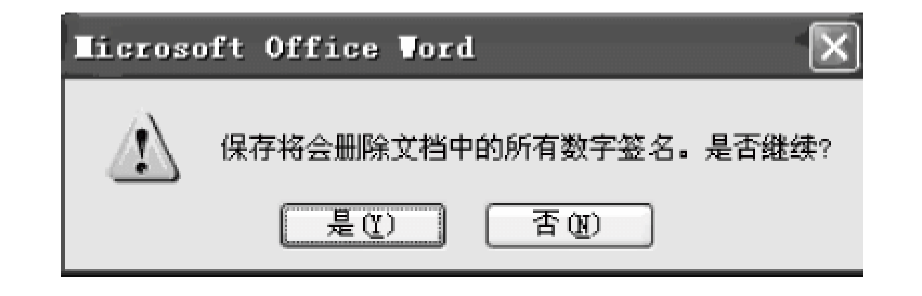


图 4.36　文档签名后的提示信息

当别人打开该文档时，选择“工具”→“选项”菜单，单击“安全性”选项卡后，在此处会看到数字证书，就知道该文档是你编写的，因为有你的数字签名。

（4）数字证书在网上银行的应用

银行数字证书的主要功能是交易方身份鉴别、保证信息的完整性和信息内容的保密性。交易方身份验证就是要能准确鉴别信息的来源，鉴别彼此通信的对等实体的身份，即银行网站验证证书持有者的身份，而客户也可以通过网站证书验证网站的合法性；保证信息的完整性就是确保收到的信息就是对方发送的信息，在交换过程中没有乱序或修改；信息内容的保密性就是对交换的信息实施加密保护，使第三者即使截获这些数据，也无法读懂其中包含的信息。

只要用户申请并使用了银行提供的数字证书，即可保证网上银行业务的安全。这样，即使黑客窃取了用户的账户密码，因为没有用户的数字证书，也就无法进入用户的网上银行账户。经过数字签名的网银交易数据是不可修改的，且具有唯一性和不可否认性，从而可以防

止他人冒用证书持有者名义进行网上交易,维护用户及银行的合法权益,减少和避免经济及法律纠纷。

数字证书申请流程通常是:用户先到银行申请数字证书→再到指定网站下载数字证书(通常是该银行网站)→下载后双击即可加载使用。下载数字证书时提示设置私钥密码,要记住该密码,因为证书导出、导入时要用到它。下载完毕后要马上导出证书把它保存好,以便在别的机器上使用。

利用 IE 浏览器导出证书的过程是:在 IE 主菜单中依次选择"工具"→"Internet 选项"→"内容"→"证书"菜单,在"个人"分类下找到颁布者为"ABC"的那个证书并选中它,单击"导出"按钮,把它存放成一个证书文件。这个文件可以存放到 U 盘中以备随时取用,也可以放在邮箱中保存。导入时只需要把保存好的证书文件复制出来,双击它就可以了。

下面以农业银行上海分行的网上银行为例,介绍银行数字证书的下载安装与应用。

个人客户若想得到网上银行的数字证书,需持本人有效身份证件及账户到银行营业网点办理证书申请手续。办理手续时填写有关电子银行业务个人客户注册申请表,选择开通网上银行服务,并签署相关的电子银行服务协议。银行营业网点将当场录入客户信息,自行设定注册密码,选择购买动态口令卡或支付宝,完成注册。注册时银行会给你一组 14 位的注册编号(授权码)和 8 位的注册密码。用户在有效期内登录到银行网站,安装根证书和申请用户数字证书。证书下载完成后,就可通过银行网站登录网上银行。

在银行网点办完证书申请手续后,用户可上网进入中国农业银行上海分行网站(http://www.95599.sh.cn)申请证书,进入如图 4.37 所示的网站首页后,首先单击右侧的"下载证书"按钮,在随后出现的页面中明确安装环境设置(操作系统);然后单击"下一步"按钮,进入"下载证书"页面,就可看到"个人用户证书下载安装"流程。按照流程首先安装 CA 根证书。



图 4.37 农行上海分行首页

① 安装 CA 根证书

中国农业银行在线银行网站公钥证书经过中国农业银行 CA 中心的根签名认证,并且

可以用中国农业银行 CA 根证书进行验证。用户安装该行的 CA 根证书后，浏览器将自动验证该行网上银行网站的有效性，避免伪造网站给用户造成损失。

安装 CA 根证书的过程如下：

第 1 步：单击安装"流程"中的"安装 CA 证书"→"CA 根证书下载"，弹出如图 4.38 所示页面。

第 2 步：单击"安装证书"按钮，弹出"证书导入向导"欢迎页面。

第 3 步：单击"下一步"按钮，弹出证书存储页面，如图 4.39 所示。



图 4.38　证书的常规信息

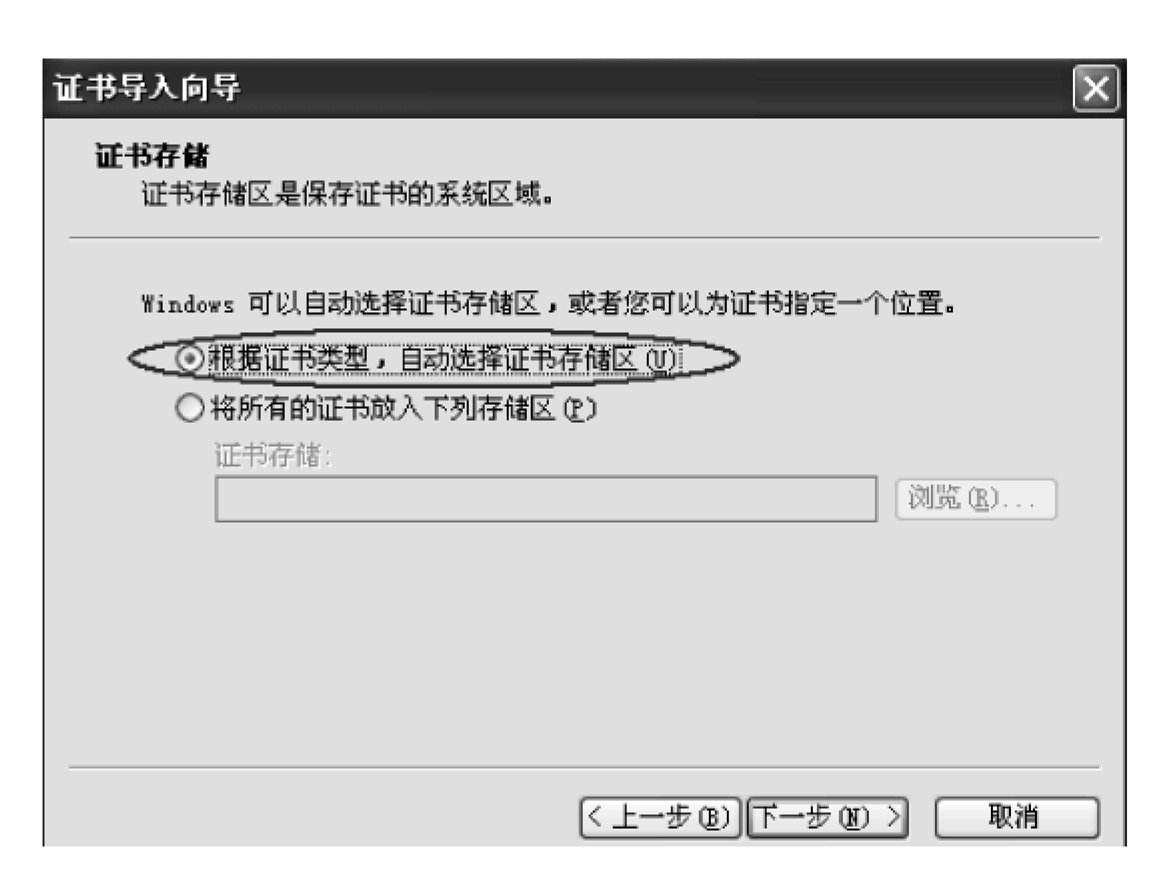


图 4.39　证书存储区域选择

第 4 步：选择"根据证书类型，自动选择证书存储区"单选项，然后单击"下一步"按钮；也可将证书下载到磁盘或 U 盘(USB)上，然后再将 CA 根证书导入 IE。

第 5 步：在出现的如图 4.40 所示页面中，单击"完成"按钮后，系统提示 CA 根证书导入成功，单击"确定"按钮，如图 4.41 所示。



图 4.40　证书导入完成



图 4.41　证书导入成功提示

② 申请数字证书

CA 根证书安装完毕后，接下来就是安装驱动程序和申请(下载安装)数字证书。安装驱动程序的过程在此不作介绍。

证书申请过程如下：

第 1 步：进入如图 4.37 所示的网站首页后，单击“下载证书”按钮。

第 2 步：单击随后出现的页面左下侧的“证书下载向导”，进入如图 4.42 所示的证书安装向导页面。

第 3 步：单击“新证书申请”，进入如图 4.43 所示的证书下载页面。

第 4 步：选择“个人注册客户”，单击“下一步”按钮，进入“个人注册客户验证”页面，如图 4.44 所示。

第 5 步：在“用户名”和“密码”框中分别输入用户名(注册编码)和密码(注册密码)，单击“下一步”按钮。

至此，即可完成证书申请。



图 4.42 安全登录证书安装向导



图 4.43 选择客户类型

③ 使用数字证书

现在，用户可以使用证书来确保网上银行的安全了。用户进入银行网站后，在“在线银行登录区”，选择“个人注册用户”，按照提示，选择正确的证书号，输入用户号和密码，即可登录自己的网上银行账户，办理转账、网上速汇通等业务。

建议在图 4.39 中选择“将所有的证书放入下列存储区”项，单击“浏览”按钮添加 U 盘(USB)，把证书保存在 U 盘上，使用网上银行时再插到计算机上，这样可有效地防止证书被盗。

USB Key(简称 UB)是一种 USB 接口的硬件设备，它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的数字证书和用户私钥。可利用 USB Key 内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中，理论上使用任何方式都无法读取，因

此保证了用户认证的安全性。由于 USB Key 的安全度高，且成本很低，所以被广泛应用于网上银行的数字证书加密。使用 USB Key 存放代表用户唯一身份的数字证书和用户私钥。在网上银行应用中，对交易数据的数字签名都是在 USB Key 内部完成的，并受到 USB Key 的 PIN 码保护。图 4.45 为银行用 USB Key 实物图。使用 USB Key 后，即使黑客完全远程控制了用户的计算机，也无法成功进行登录认证交易。





图 4.44 验证用户信息



图 4.45 银行用 USB Key 实物图

提示：当个人客户使用 USB Key 作为证书存放介质时，必须安装 USB Key 驱动程序，安装完成后再进行证书申请。

4.4.3 Office 2003/XP 文档的安全保护

Word 和 Excel 是人们日常工作和生活中十分常用的办公软件，因此，保证 Word 和 Excel 文档的安全是十分重要的。Word 和 Excel 本身也提供了许多安全和保护功能。本节介绍几种对 Word 和 Excel 文档实现安全保护的技巧。

1. 保护文档的保密性

如果用户不希望自己的 Word 和 Excel 文档被别人阅读，可以通过添加"打开密码"方式实施保护。可以有如下方法为 Word 文档添加密码。

(1) 启动 Word，打开需要加密的文档，单击"工具"→"选项"命令，打开"选项"窗口，单击"安全性"选项卡，如图 4.46 所示；在图中"打开文件时的密码"右侧的方框中输入密码，单击"确定"按钮，随后再输入一次该密码，单击"确定"按钮退出，然后保存当前文档即可。

注意：上述"加密"设置并非对文档内容进行了加密，而是为打开该文档设置了"密码"。此后需要打开该文档时，需要输入正确的密码，否则不能打开文档。

(2) 在对新建文档进行"保存"或对原有文档进行"另存为"操作时，打开"文件"菜单，选择"另存为"，在弹出的"另存为"窗口的右上角点开"工具"菜单项，在其下拉菜单中选择"安全性措施"选项，弹出如图 4.47 所示的"安全性"对话框，其后步骤同方法(1)。

实际上，这两种方法是一样的，只是操作步骤不同而已。

可以用类似方法操作为 Excel 文档设置密码保护。方法(2)中稍有不同的是：在出现的"另存为"窗口的右上角点开"工具"菜单项，在其下拉菜单中选择"常规"选项而非"安全性措施"选项，弹出如图 4.48 所示对话框。

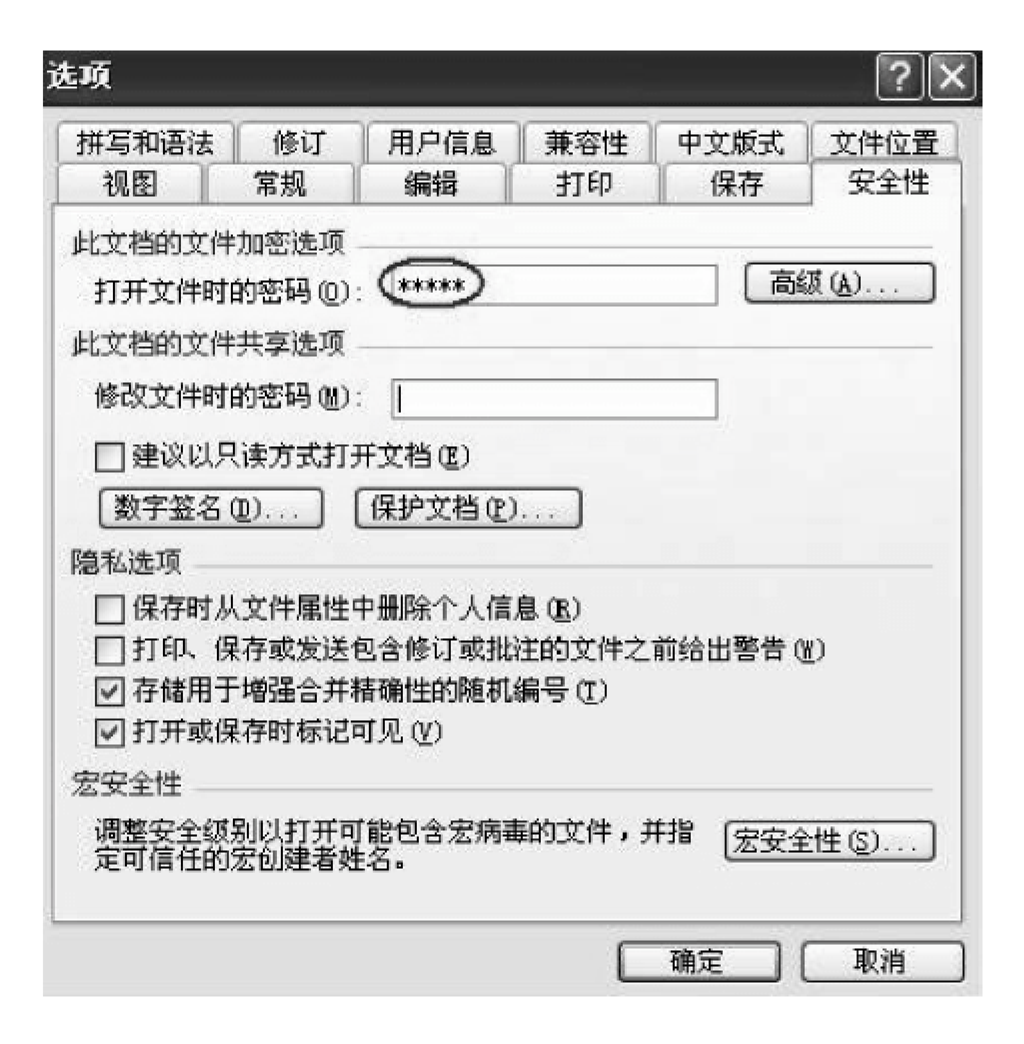


图 4.46 设置打开文档密码(1)



图 4.47 设置打开文档密码(2)

2. 保护 Word 文档的完整性

如果用户的 Word 和 Excel 文档允许别人查看而不允许修改，可以采取设置“修改密码”的方法实现。

在图 4.46 或图 4.47 “修改文件时的密码” 或图 4.48“修改权限密码”右侧的方框中输入密码，单击“确定”按钮，再输入一次确认密码，单击“确定”按钮退出后，保存当前文档。这样可使别人阅读相关文档而不能对其进行编辑。

注意：在打开设置了“修改文件时的密码”的文档时，会弹出如图 4.49 所示对话框。如在对话框中输入密码，则可打开 Word 文档并进行编辑和修改；如不输入密码，直接单击左侧下方的“只读”按钮，则可打开 Word 文档进行浏览，但此时对文档所作的任何修改，均不能被保存到原文档中。

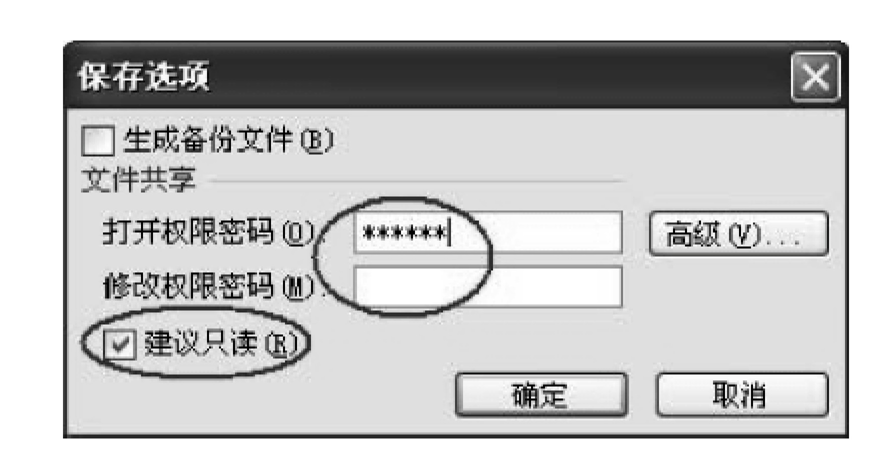


图 4.48 设置打开文档密码(3)

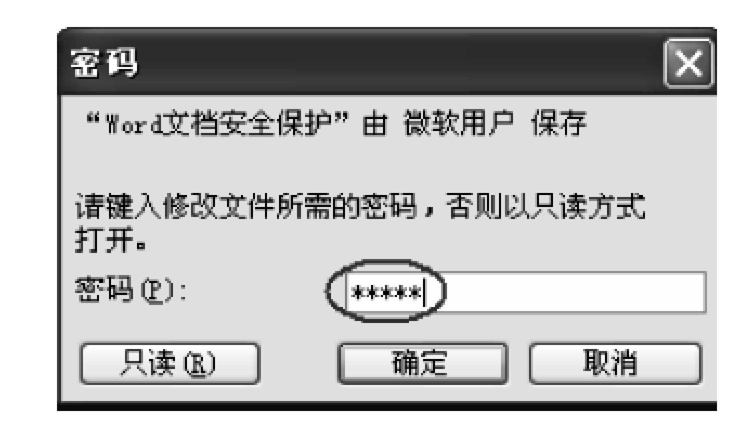


图 4.49 输入修改文件密码

在 Excel 环境下，勾选图 4.48 所示对话框的“建议只读”复选框，这样无论何时打开工作簿，Excel 总是首先显示出一个提示信息对话框，建议应以只读方式打开工作簿，达到工作簿内容不被改写的目的。

设置“打开文件时的密码”是为了防止别人修改 Word(或 Excel)文档，对文档起保密作用。如果只设置“修改密码”，那么别人仍然可以打开该文档(如只读方式)，但是若不知道密码，则不能对其做任何修改，这可起到保护文档完整性作用。这两种密码是相互独立的，可以根据自己的需要分别设定，它们可以相同也可以不同。

3. 禁止未授权编辑文档

(1) 保护 Word 文档

在 Word 文档中选择“工具”→“保护文档”命令(或在图 4.46、图 4.47 中单击“保护文档”按钮),在编辑文档的右侧展开“保护文档”任务窗格,如图 4.50 所示。勾选“仅允许在文档中进行此类编辑”项后,其下面的对话框中有 4 个可选项:未作任何更改(只读)、填写窗体、批注和修订。选择“未作任何更改(只读)”项表示“文档受密码保护,特殊限制有效,只能查看此区域”;选择“填写窗体”项表示“文档受密码保护,特殊限制有效,只能在此区域中填写窗体”;选择“批注”项表示“文档受密码保护,特殊限制有效,只能在此区域中插入批注”;选择“修订”项表示“文档受密码保护,特殊限制有效,可以在此区域中编辑,但所有更改将作为修订”。选择上述四项之一(如“填写窗体”,见图 4.51)后单击“是,启动强制保护”按钮,打开如图 4.52 所示的“启动强制保护”对话框。输入密码并再次输入确认密码,单击“确定”按钮返回。

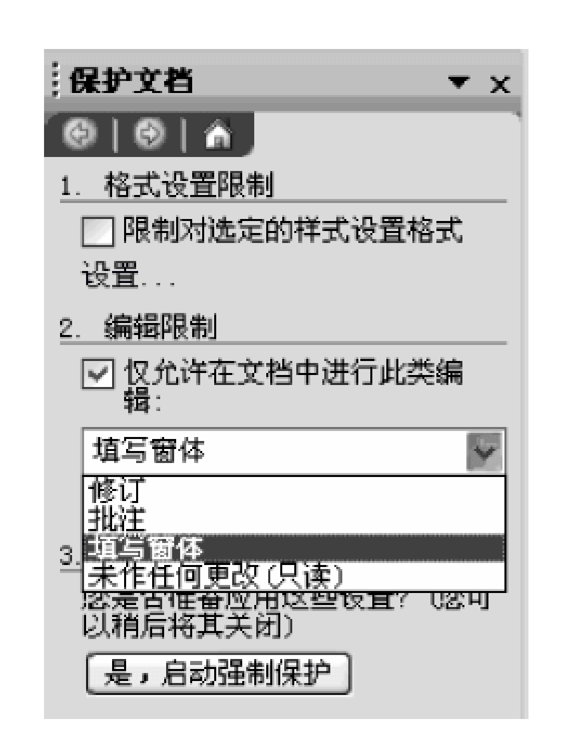




图 4.50　设置保护文档的编辑限制(1)

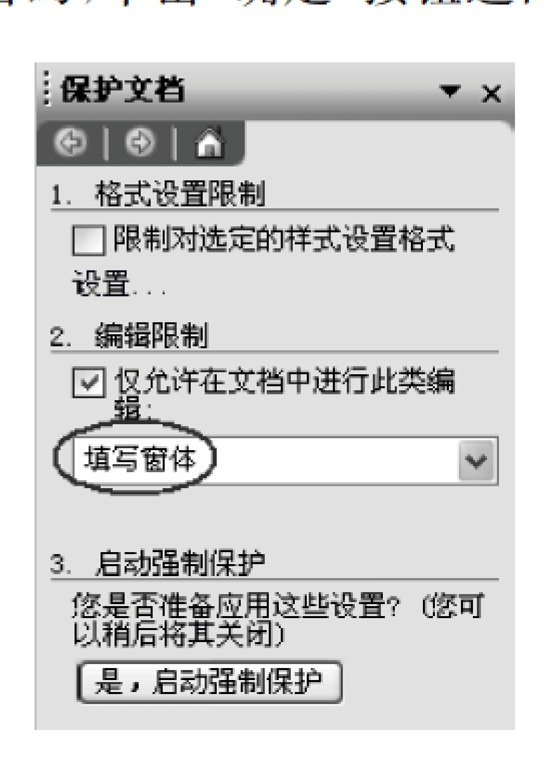


图 4.51　设置保护文档的编辑限制(2)

当 Word 文档需要传给不同的人查看,希望对方添加批注而不希望其进行其他编辑时,可以在图 4.50“保护文档”窗口中选择“仅允许在此文档中进行此类编辑”中的“批注”,这样别人就只能对文档进行批注,而无法进行其他操作;如果希望对文档进行修订,则可选择“修订”项,此时对文档所做的编辑更改只能作为“修订”;如果只希望别人阅读此文档而不允许进行任何修改,则可选择“未作任何更改(只读)”项。

对 Word 文档“启动强制保护”后,工具栏和格式的大部分设置(工具按钮)都变为浅灰色,不能被操作,这就说明设置的保护已经生效了。

如果需要重新编辑或修改文档时,要解除上述保护,可选择“工具”→“取消文档保护”命令,在弹出的如图 4.53 所示的密码框中输入正确的密码,单击“确定”按钮即可。

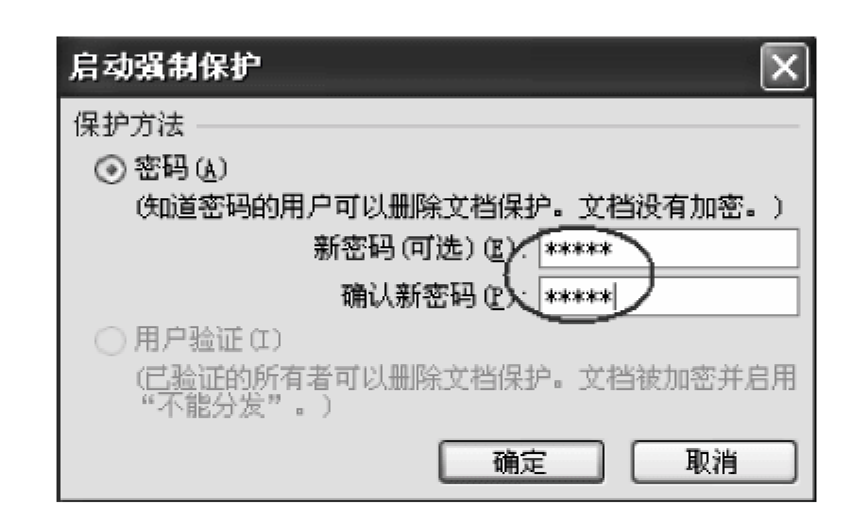


图 4.52　启动强制保护时设置密码



图 4.53　取消文件保护时输入密码

(2) 保护 Excel 文档

在 Excel 工作表中，选定需要锁定的单元格，选择"格式"→"单元格"菜单(或选中并右击单元格，在弹出的菜单中选择"设置单元格格式"项)，在"单元格格式"设置对话框中选择"保护"选项卡，并选中"锁定"(默认状态下单元格和图形对象均处于锁定状态)；执行"工具"→"保护"→"保护工作表"命令，设置保护密码，即完成对单元格的锁定设置。此时，已设置了工作表保护，工作表中相应信息不能被修改。如果要防止其他用户取消工作表保护，可在"密码"文本框中输入密码并再次确认，如图 4.54 所示。

当用户想撤销所做的工作表保护时，在 Excel 工作表中，选择"工具"→"保护"→"撤销工作表保护"命令即可。

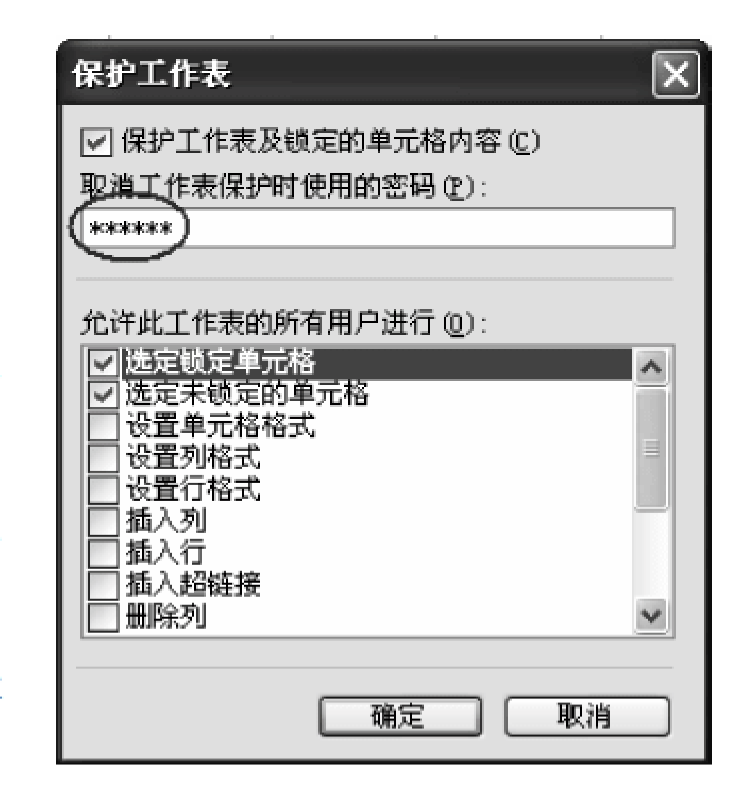


图 4.54 设置保护工作表密码

4. 隐藏文档记录

在一台微机可能被多个用户使用的情况下，如果用户 A 在该机上编辑并保存 Word 或 Excel 文档后下机，当用户 B 再使用该机时，就有两种渠道查看到用户 A 编辑过的 Word 或 Excel 文件名：一种是在"开始"菜单的"文档"下；另一种是在打开 Word 或 Excel 文档后的"文件"菜单下。如果用户 A 的这些文件或其存储的位置在上次使用退出后未做改变，则用户 B 单击相应的文件名就可打开文件，并可进行阅读和修改。通常情况下用户不希望别人阅读、修改或复制自己编辑过的文件，因此用户要设法保护自己的文件。可采取如下操作保护 Word 或 Excel 文档不被其他人打开。

(1) 对于第一种情况，可有如下两种方法。

方法 1：用户可在"开始"→"运行"框中输入"gpedit.msc"并确认，打开组策略，依次打开"用户配置"→"管理模板"→"任务栏和「开始」菜单"，如图 4.55 所示。然后在右边的设置列表中进行操作，以下两种操作均可达到目的。

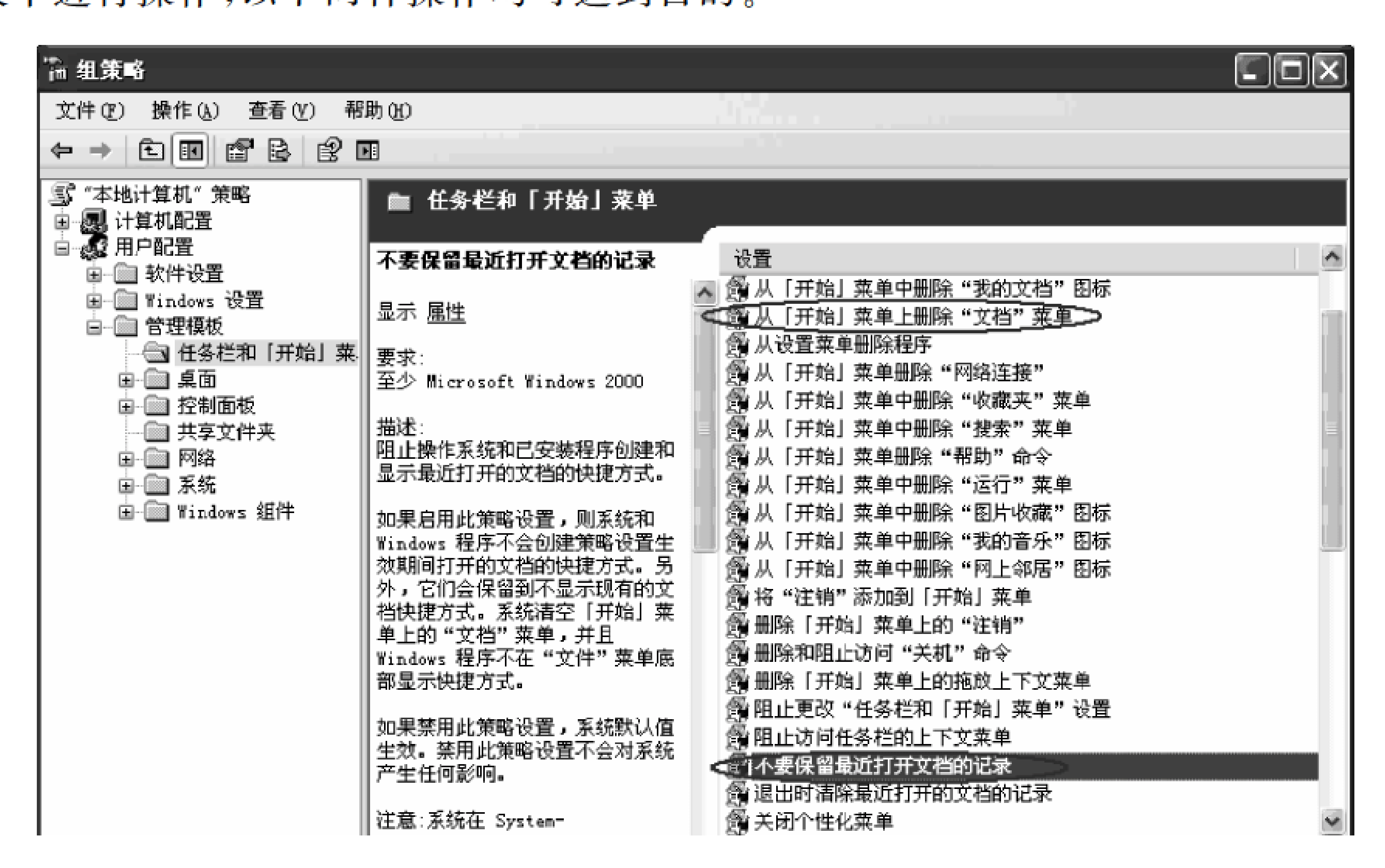


图 4.55 组策略之"任务栏和「开始」菜单"

① 在图 4.55 中选择“从「开始」菜单上删除‘文档’菜单”项，双击打开后，选择“已启用”选项，如图 4.56 所示，再单击“确定”按钮。这样做的结果可以使“开始”菜单中的“我最近的文档”项彻底消失。

② 在图 4.55 中选择“不要保留最近打开文档的记录”项，双击打开后，选择“已启用”选项，如图 4.57 所示，再单击“确定”按钮。这样做后用户最近打开过的所有文档的记录都不再出现。

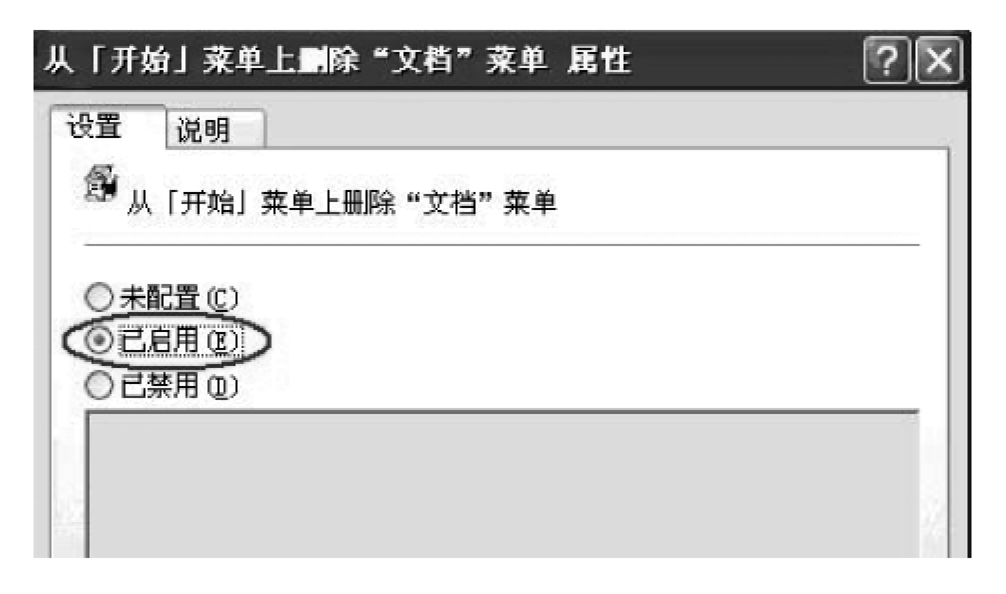


图 4.56　“从「开始」菜单上删除‘文档’菜单 属性”对话框

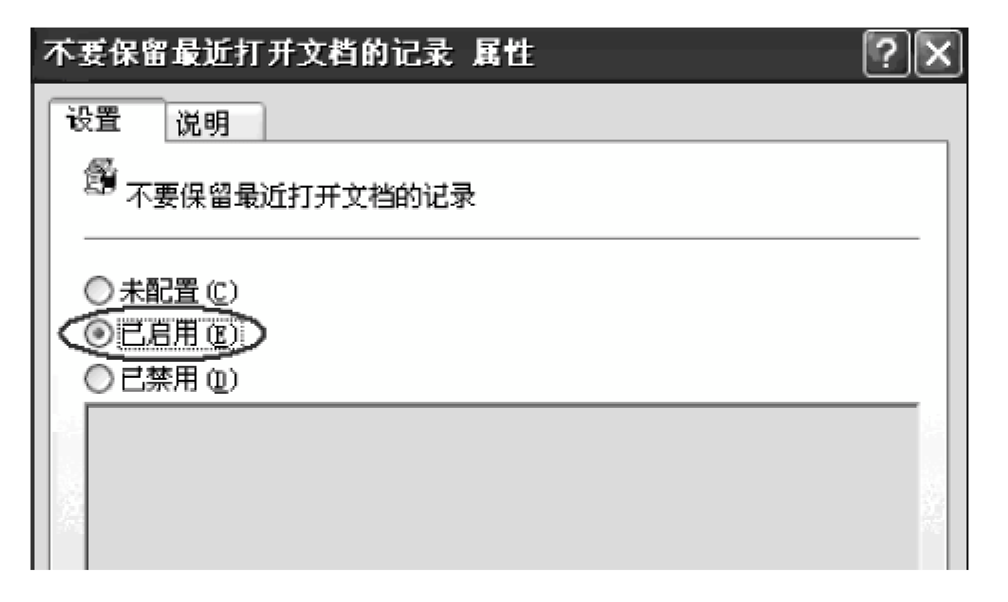


图 4.57　“不要保留最近打开文档的记录 属性”对话框

方法 2：右击“开始”命令，选择“属性”，在“任务栏和「开始」菜单 属性”对话框中选“「开始」菜单”选项卡，选中“「开始」菜单”，单击“自定义”按钮，在弹出的图 4.58 所示的“自定义「开始」菜单”对话框中选择“高级”选项卡，取消最下端“列出我最近打开的文档”复选框的选择，单击“清除列表”按钮，如图 4.58 所示。完成上述操作后再查看“开始”→“文档”下即为“(空)”了。



图 4.58　自定义“开始”菜单

(2) 对于第二种情况，用户可在 Word 或 Excel 环境下，执行“工具”→“选项”命令，打开“常规”选项卡，取消“列出最近所用文件”或“最近使用的文件列表”复选框的选择(或将文件数字降为 0)即可，如图 4.59 和图 4.60 所示。

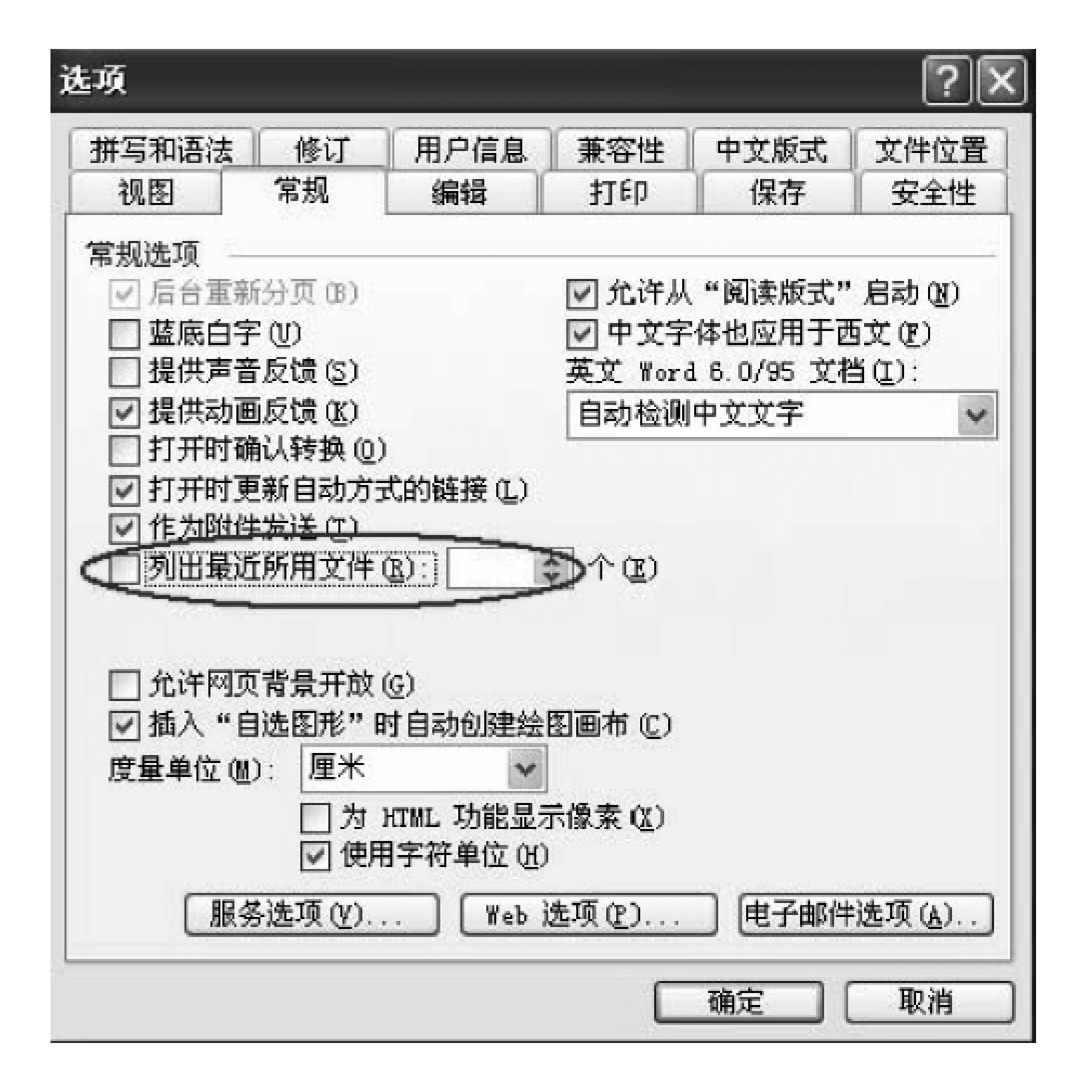


图 4.59　Word 下取消"列出最近所用文件"

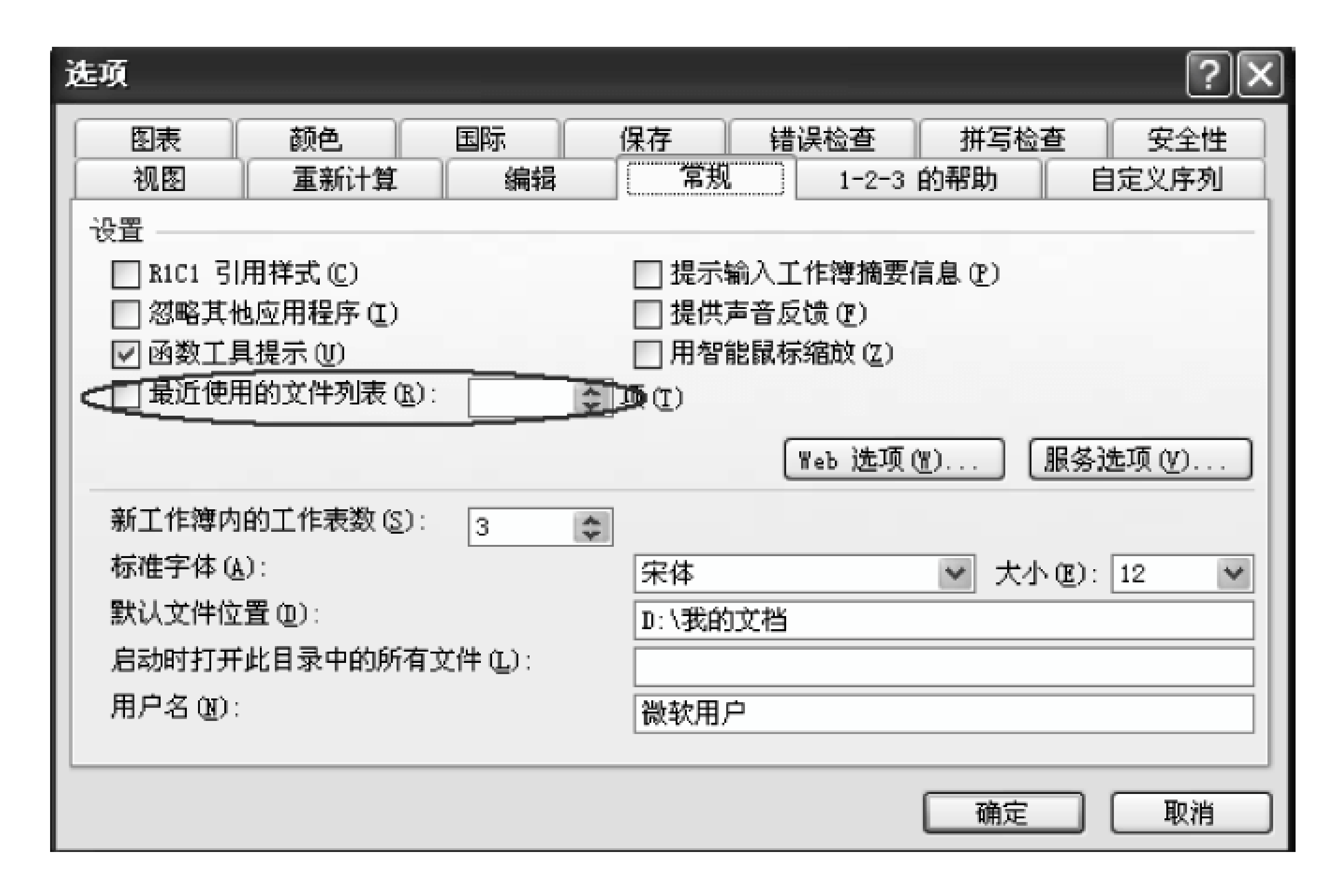


图 4.60　Excel 下取消"最近使用的文件列表"

5. 宏病毒防范

Word 和 Excel 提供了对宏病毒的警告保护,用户可以选择"工具"→"宏"→"安全性"菜单,在弹出的对话框中设置各种安全级别。建议设置为"高"或"中",如图 4.61 所示。使禁止非可靠来源文档中宏的运行,或在运行前给出警告提示,让用户选择运行与否。需提醒的是这样做只能从一定程度上预防宏病毒而不能杀毒,所以要真正杜绝宏病毒,还应该使用防病毒软件。

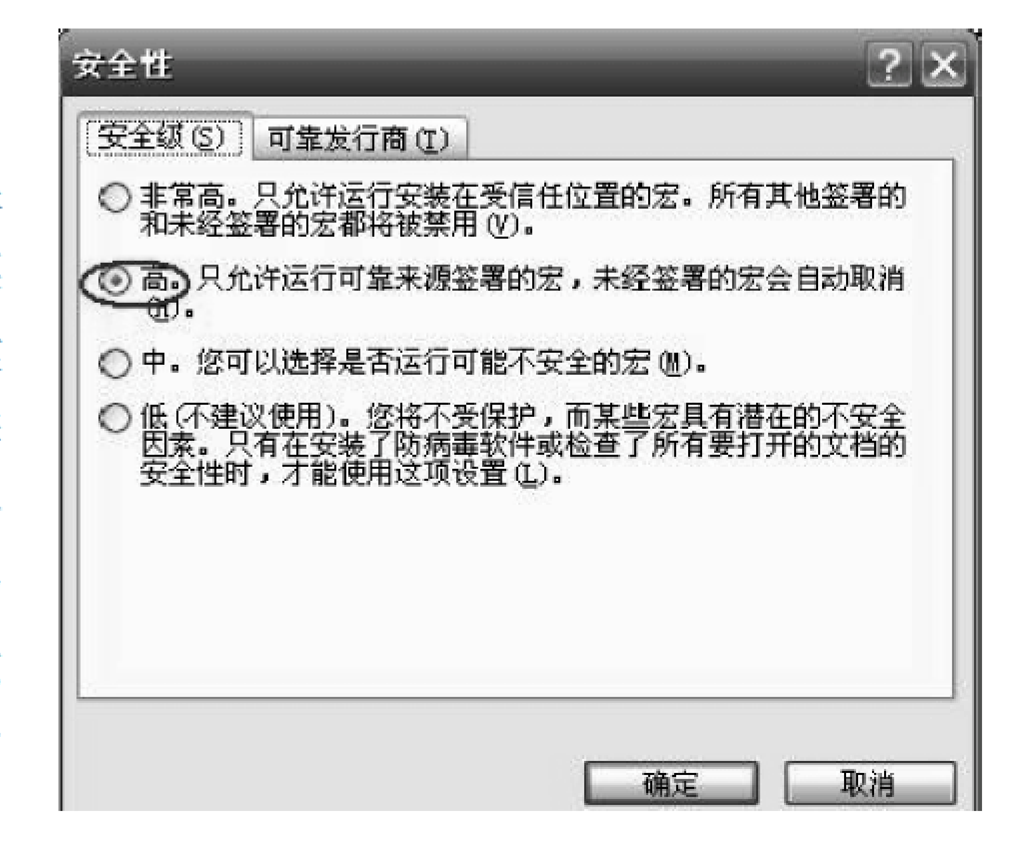


图 4.61　设置安全性级别

6. 突发事件下的文档保存和备份

（1）文档自动保存

用户在编辑文档时，当编辑很多内容没有及时保存，或因其他事情离开机器，或在机器上转而执行其他操作时，如遇到突然停电或非正常关机等突发事件，重启机器后原来编辑过的内容可能就会丢失或部分损坏。可利用 Word 和 Excel 提供的“自动保存”功能来避免这样的损失。

在 Word 环境下，选择“工具”→“选项”→“保存”菜单，勾选“自动保存时间间隔”复选框，在“分钟”文本框中选定希望自动保存的时间间隔（如 8 分钟），如图 4.62 所示。

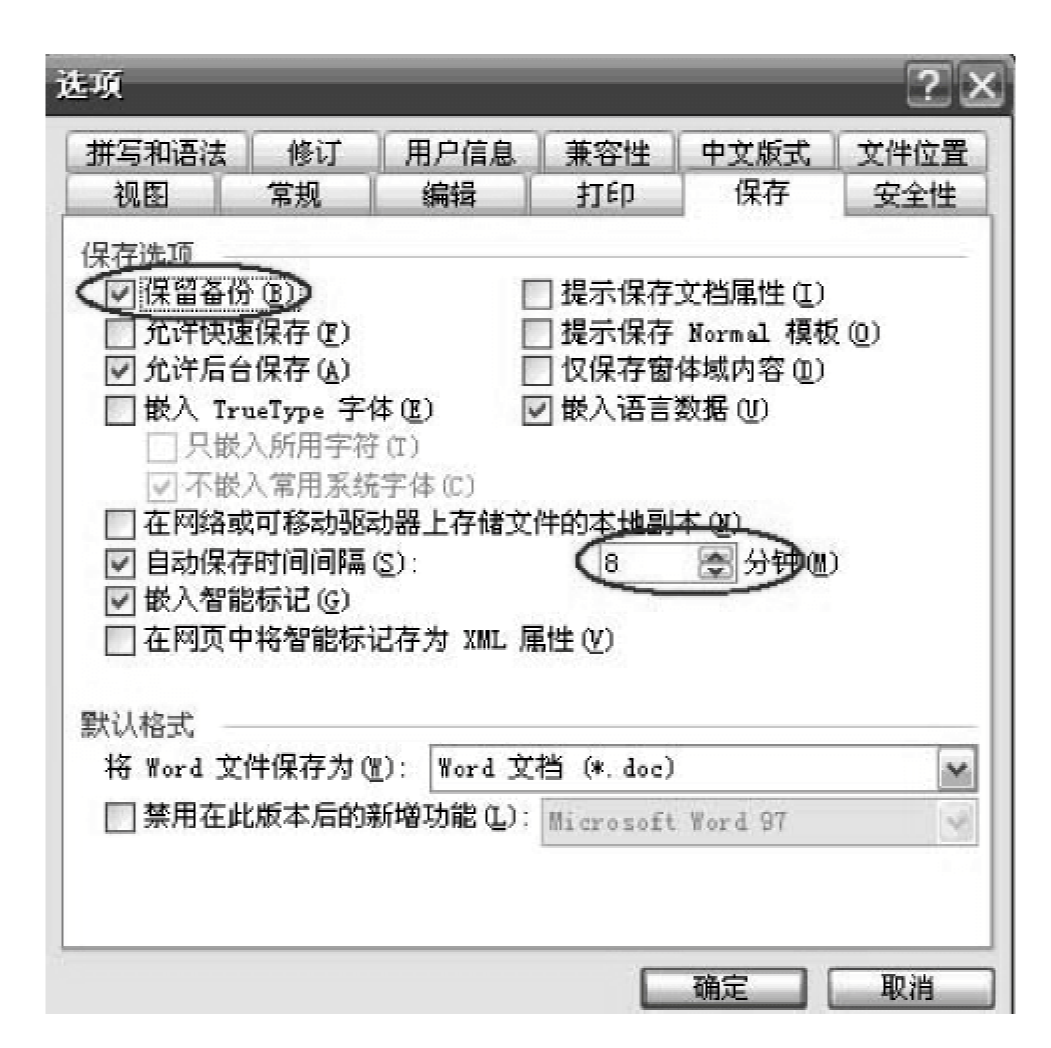


图 4.62　设置 Word 自动保存时间和自动备份

在 Excel 环境下，首先单击“工具”菜单中的“加载宏”命令，弹出“加载宏”对话框，在“当前加载宏”列表框中找到并选中“自动保存”复选框，单击“确定”按钮返回；然后选择“工具”→“选项”→“保存”选项，选中“保存自动恢复信息，每隔”复选框，在“分钟”文本框中输入希望 Excel 自动保存工作簿的时间间隔（如 7 分钟），如图 4.63 所示。

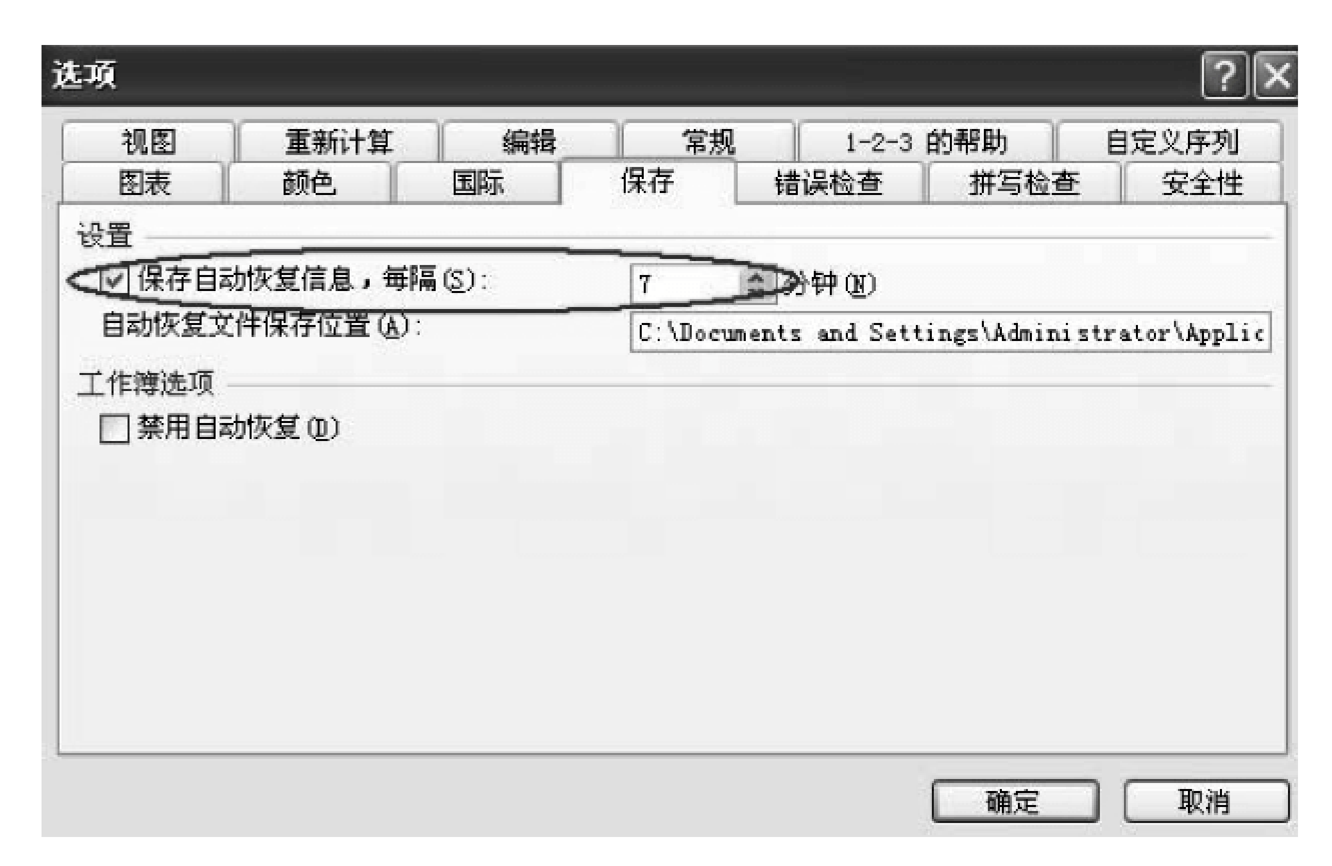


图 4.63　设置 Excel 自动保存时间

不要把间隔时间设置得太短，否则频繁地保存既浪费时间，又损伤硬盘；但该时间也不能设置得太长，否则就起不到保护作用了。设置好后，再碰到突发情况，文档就可恢复到最后一次保存的状态。

（2）文档备份

Word 还提供了文档备份功能，其操作过程为：选择"工具"→"选项"→"保存"菜单中的"保留备份"选项，如图 4.62 所示。这样，在将当前的修改内容保存到原文档的同时，还保存到备份文件中。如在 Office XP 下原文件名为"abcde"(其类型为"Microsoft Word 文档")，在保存原文件后，还会出现一个文件名为"备份属于 abcde"的文件(其类型为"Microsoft Word 备份文档")。

Excel 也提供了文档自动备份功能，其操作过程为：在选择"开始"→"另存为"→"工具"→"常规选项"后弹出的图 4.48 窗口中，勾选左上角的"生成备份文件"复选框，单击"确定"按钮。这样就可以在文档保存目录下生成一个备份文件。

7. 为文档签名

为防止编写好的 Word 文档被别人进行恶意的修改，可对其进行保密设置。除上述设置"打开密码"外，还可以使用数字签名对其进行保护。用户可选择下载安装数字签名软件对文档进行签名，onSign 就是一款优秀的、通过运行宏为 Word 文档添加数字签名的软件。在此处就不再对 onSign 软件的下载、安装及应用方法进行介绍了，用户可参考其他资料。用户还可以选择利用数字证书方式对文档进行签名，参见 4.4.2 节。

8. Excel 文档的其他保护措施

（1）保护工作簿结构及共享

在当前工作簿下，选择"工具"→"保护"→"保护工作簿"命令；勾选"结构"项，单击"确定"按钮后即可保护工作簿结构不被删除、移动、隐藏、取消隐藏和重命名工作表，并且不可插入新的工作表，如图 4.64 所示。若勾选"窗口"项并确认后，可以保护工作簿窗口不被移动、缩放、隐藏、取消隐藏或关闭。

对要共享的工作簿，如果要对工作簿中的修订进行跟踪，可设置保护共享工作簿。其操作为：选择"工具"→"保护"→"保护共享工作簿"命令，勾选"以追踪修订方式共享"复选框，如图 4.65 所示。如果需要其他用户先提供密码才能取消共享保护和冲突日志，则需要在"密码"文本框中输入密码。如果工作簿已经处在共享状态，则不能为其设置密码。



图 4.64 Excel 保护工作簿设置



图 4.65 Excel 保护共享工作簿设置

(2) 隐藏工作簿和工作表

在当前工作簿下，选择“窗口”→“隐藏”命令，可以把当前处于活动状态的工作簿隐藏起来；如果要取消隐藏，可执行“窗口”→“取消隐藏”命令，然后在“取消隐藏”窗口中选择相应工作簿即可。

在一个工作簿中有多个工作表的情况下，可在当前工作表下，选择“格式”→“工作表”→“隐藏”命令，即可把当前的活动工作表隐藏起来；要取消工作表的隐藏时，选择“格式”→“工作表”→“取消隐藏”命令，然后在“取消隐藏”窗口中选择相应的工作表即可。

(3) 隐藏工作表的行或列

如果在打印工作表时不希望打印某行或某列，或者不希望有权查看工作表的人看到某行或某列内容，但仍需保留这些内容时，可将这些行或列隐藏起来，需要时再恢复出来。隐藏 Excel 工作表行或列有如下三种简单方法。

① 选定要隐藏的行(列)并右击之，在出现的快捷菜单中选择“隐藏”命令。

② 单击要隐藏行(列)中的任意单元格，选择“格式”菜单下的“行”(“列”)→“隐藏”命令。

③ 将鼠标放在要隐藏行(列)号码的下(右)侧格线上，按住左键向上(左)移动鼠标，将行(列)宽调整为 0，这样对应的行(列)号就从工作表中自动消失，起到隐藏效果。

若要取消隐藏，先要同时选择该行(列)的上下(左右)相邻两行(列)，或者选中整个工作表，再选择“格式”菜单下的“行”(“列”)→“取消隐藏”命令即可。

(4) 对单元格输入信息进行有效性设置

在当前工作表下，首先选定要进行有效性检测的单元格或单元格集合，然后选择“数据”菜单中的“有效性”选项，弹出如图 4.66 所示对话框；再分别对“设置”标签的“有效性条件”、“输入信息”和“出错警告”标签的相关项进行设定，以控制输入单元格的信息使之符合给定的条件。这些设置很有用，如在设计 Excel 时，可做到不允许用户输入负数年龄、负数工资，以及个数、人数、次数中不出现小数等现象。

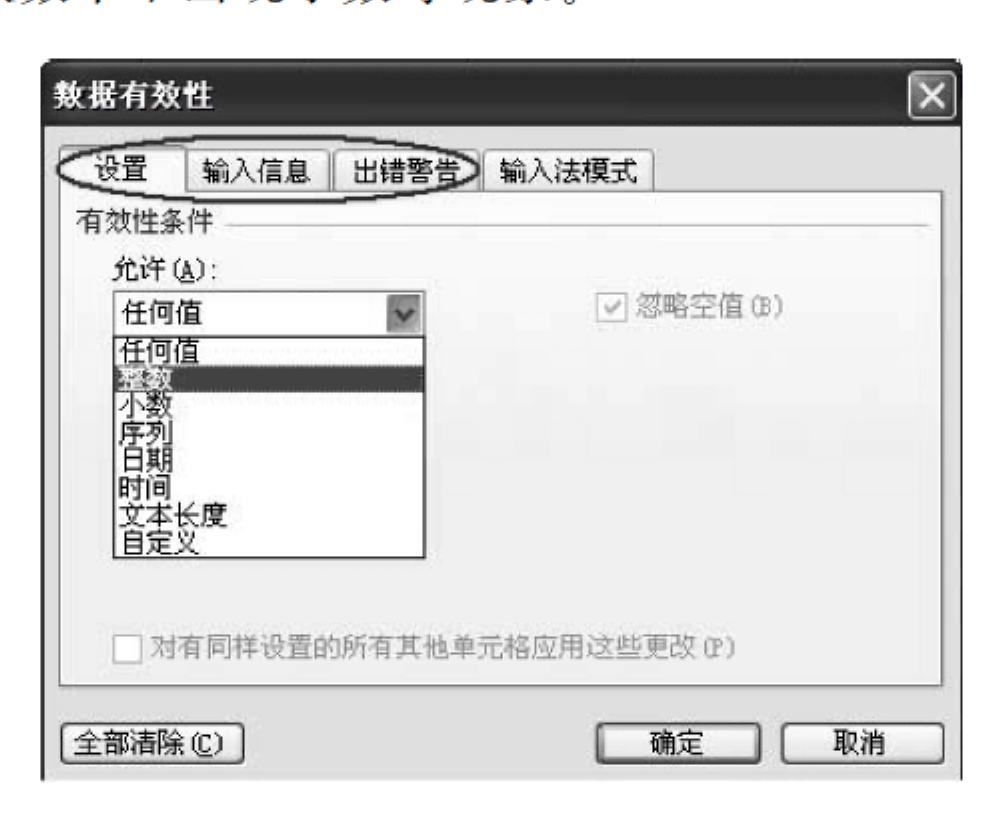


图 4.66　Excel 单元格有效性设置

习题和思考题

一、问答题

1. 简述密码学的两方面含义。

2. 什么是加密、解密、密钥和密码算法？

3. 一般的密码系统由哪几部分组成?

4. 什么是分组密码和序列密码?

5. 什么是移位密码和替代密码? 举例说明。

6. 简述对称密钥密码和非对称密钥密码体制及其特点。

7. 简述数字签名的概念及其功能。

8. 简述不安全的口令表现。如何保持和维护口令安全?

9. 简述数字证书的功能和应用。

二、填空题

1. 把明文变换成密文的过程叫(　　);解密过程是利用解密密钥,对(　　)按照解密算法规则变换,得到(　　)的过程。

2. 典型的对称密钥密码算法有(　　)、(　　)和(　　)等。

3. 典型的非对称密码算法有(　　)、(　　)和(　　)等,它们的安全性都是基于(　　)。

4. 在密码算法公开的情况下,密码系统的保密强度基本上取决于(　　)。

5. IDEA 是(　　)密码体制的算法。它使用(　　)位密钥可对(　　)位的分组进行加密和解密。

6. 密码学包括(　　)和(　　)两部分,其中(　　)研究的是通过(　　)来改变(　　)的形式,使得编码后的信息除(　　)之外的其他人都不可理解;(　　)研究的是如何(　　),恢复被隐藏起来信息的(　　)。(　　)是实现对信息加密的,(　　)是实现对信息解密的,这两部分相辅相成,互相促进,也是矛盾的两个方面。

7. 用户身份验证一般涉及两个过程:(　　)和验证。验证是指(　　),验证信息一般是(　　)。

8. DES 的加密算法和解密算法(　　)。

9. 对称加密体制与非对称加密体制相比具有(　　)的优点。

10. PGP 使用混合加密算法,它是由一个对称加密算法(　　)和一个非对称加密算法(　　)实现数据的加密。PGP 软件具有(　　)和(　　)两种功能。在 PGP 中,主要使用(　　)算法对数据进行加密,使用(　　)算法对密钥进行加密。它不但可以对用户的(　　),以防止非授权者阅读,还能对邮件进行(　　),使收信人确信邮件未被第三者篡改。

11. 广泛应用的数字签名的算法主要有(　　)、(　　)和(　　)。

12. 通过数字签名和数字证书技术可实现交易的(　　)性。

13. 20 世纪 70 年代,密码学的两大成果分别是(　　)和(　　)。前者将传统的密码学发展到了一个新的高度,后者的提出被公认为是实现现代密码学的基石。这两大成果已成为近代(　　)发展史上两个重要的里程碑。

三、单项选择题

1. 最著名、应用最广泛的非对称密码算法是(　　),它的安全性是基于大整数因子分解的困难性。

A. DES　　B. RSA　　C. 3DES　　D. DSA

2. 最典型的对称密钥密码算法是(　　),它是用 56 位密钥对 64 位明文(密文)进行加密(解密)的。

A. DES　　B. RSA　　C. 3DES　　D. DSA

3. 在加密时将明文中的每个或每组字符由另一个或另一组字符所替换,原字符被隐藏起来,这种密码称为( )。

A. 移位密码 B. 分组密码 C. 替代密码 D. 序列密码

4. 如果加密密钥和解密密钥相同或相近,这样的密码系统称为( )系统。

A. 对称密钥 B. 非对称密钥 C. 公钥密码 D. 分组密码

5. DES 算法一次可用 56 位密钥组把( )位明文(或密文)组数据加密(或解密)。

A. 32 B. 48 C. 64 D. 128

6. 以下( )项要求不是数字签名技术可完成的目标。

A. 数据保密性 B. 信息完整性 C. 身份验证 D. 防止交易抵赖

7. 在 RSA 算法中,取密钥 e=3,d=7,则明文 6 的密文是( )。

A. 18 B. 19 C. 20 D. 21

8. 在 RSA 算法中,取密钥 e=3,d=7,则明文 4 的密文是( )。

A. 28 B. 29 C. 30 D. 31

9. CA 认证中心不具有( )功能。

A. 证书的颁发 B. 证书的申请 C. 证书的查询 D. 证书的归档

10. 使用数字证书可实现( )。

A. 数据加密 B. 保护信息完整 C. 防止交易抵赖 D. A、B、C 都对

四、实验题

1. PGP 软件应用实验:下载、安装 PGP 软件,选择密钥;用 PGP 软件对一个要在 Internet 上传输的 Word 文档或邮件进行加密、签名,再进行解密、验证。

2. 对称数据加密实验:选一款数据加解密软件(如 DES、TDES 或 IDEA),下载安装后运行;对自己了解其内容的文件进行对称加密;加密后浏览加密文件的内容;再对加密文件进行解密(恢复原文件)后再浏览其内容。

3. 数字签名实验:在某网站上申请数字证书,并使用其对文件进行数字签名。

4. 文档加密实验:对编辑好的 Word 文件和 Excel 文档进行加密和解密操作。

第5章 软件安全技术与应用实践

软件安全(software security)就是使软件在受到恶意攻击的情形下依然能够继续正确运行的工程化软件思想,也有一些专家和学者将"软件安全"称为"软件确保"。

5.1 软件安全策略

5.1.1 软件限制策略及应用

在企业网络管理中,可利用域控制器实现对某些软件的使用限制。当用户利用域账户登录到工作电脑的时候,系统会根据这个域账户的访问权限,判断其是否有某个应用软件的使用权限。当确定其没有相关权限时,操作系统就会拒绝用户访问该应用软件,从而来管理企业员工的操作行为,这就是域环境中的软件限制策略。

1. 软件限制策略原则

(1) 应用软件与数据文件的独立原则

在使用软件限制策略时,应坚持"应用软件与数据文件独立"的原则,即用户即使具有数据文件的访问权限,但若没有其关联软件的访问权限,仍然不能打开这个文件。比如某个用户从网上下载了一部电影,虽然他作为所有者具有对该数据文件进行访问的权限,但软件限制策略限制了该用户账户对任何视频播放软件都无法访问,这样,该用户仍然无法播放这部电影。

这就是应用软件与数据文件独立的原则,该原则在实际应用中非常有用。因为很难控制用户从网络上下载文件,如用户可从网络上下载歌曲,甚至通过 U 盘等移动存储介质从企业外部把文件复制到内部计算机中,这些行为很难控制。但是可以做到对用户的应用程序进行控制,因为只需把这些应用程序控制好,即使用户私自下载了受限制的文件,用户最终也不能打开它。

(2) 软件限制策略的冲突处理原则

软件限制策略与其他组策略一样,可以在多个级别上进行设置,即可将软件限制策略看成是组策略中的一个特殊分支。所以,软件限制策略可以在本地计算机、站点、域或组织单元等多个环节进行设置。每个级别又可以针对用户与计算机进行设置。

当在各个设置级别上的软件限制策略发生冲突时,应考虑优先性问题。一般来说,其优

先性的级别从高到低为组织单元策略、域策略、站点策略和本地计算机策略。这就是说组织单元策略要比域策略的优先级高。如在域策略中限制用户使用视频播放器，而在一个组织单元中可允许该单元中的账户具有视频软件的访问权限，即使这个组织单元在这个域中，只要账户属于这个组织单元，则其仍然可以使用视频软件。

最好把软件限制策略设定在域中与组织单元中，而不是其他两个级别。在域中，实现一些共有的配置，如限制企业员工使用 QQ 或 MSN 聊天工具等。而在组织单元中，一般情况下继承域的相关配置，这样就可以保证有一个比较统一的软件权限策略管理平台。若设置级别太多，特别是在本地计算机上配置，则会破坏这个统一平台。

(3) 软件限制的规则

默认情况下，软件限制策略提供了不受限的和不允许的两种软件限制规则。

不受限的规则规定所有登录的用户都可以运行指定的软件。只要用户具有数据文件的访问权限，就可以利用软件打开这个文件。因此，应用软件的访问权限与数据文件的访问权限是独立的。用户只具有应用软件或数据文件的访问权限往往还不够，只有当两者权限都有，才能够打开相关的文件。

不允许的规则规定所有登录系统的账户都不能运行这个应用软件，无论其是否对数据文件具有访问权限。

系统默认的策略是所有软件运行都是不受限的，即只要用户对于数据文件有访问权限，就可以运行对应的应用软件。

2. 软件限制策略的应用

企业的网络管理员一般都遇到过这种困扰，老板不希望员工在工作时间用 QQ 聊天或玩游戏，但总有员工会私下安装被禁止的软件。如果使用监控软件进行监视，这样就有侵犯隐私之嫌；如果客户端是 Windows XP Professional，使用其中的软件限制策略即可达到目的。

简单来说，软件限制策略是一种技术，通过这种技术，管理员可以决定哪些程序是可信赖的，哪些是不可信赖的。对于不可信赖的程序，系统会拒绝执行。通常，管理员可以让系统使用文件路径、文件 Hash 值、文件证书、文件被下载的网站在 Internet 选项中的区域、特定扩展名文件，以及其他强制属性等方式鉴别软件是否可信赖。

软件限制策略不仅可以在单机的 Windows XP 操作系统中设置，还可以通过域对所有加入该域的客户端计算机进行设置，并可以设置影响某个特定用户或用户组，或所有用户。另一方面，可能因为错误的设置而导致某些系统组件无法运行(如禁止运行所有 msc 后缀的文件而无法打开组策略编辑器)，这样，只要重新启动系统到安全模式，然后使用 Administrator 账号登录并删除或修改这一策略即可。因为安全模式下使用 Administrator 账号登录是不受这些策略影响的。现以单机形式进行说明，并设置影响所有用户。

假设员工的计算机仅可运行操作系统自带的所有程序(C 盘)和工作所必需的 Word、Excel、PowerPoint 和 Outlook，并假设 Office 程序安装在 D 盘，员工电脑的操作系统为 Windows XP Professional。

运行 Gpedit. msc 打开组策略编辑器，可以发现有“计算机配置”和“用户设置”条目，如图 5.1 所示。如果希望对本地登录到计算机的所有用户生效，则使用“计算机配置”下的策

略；如果希望对某个特定用户或用户组生效，则使用“用户配置”下的策略。

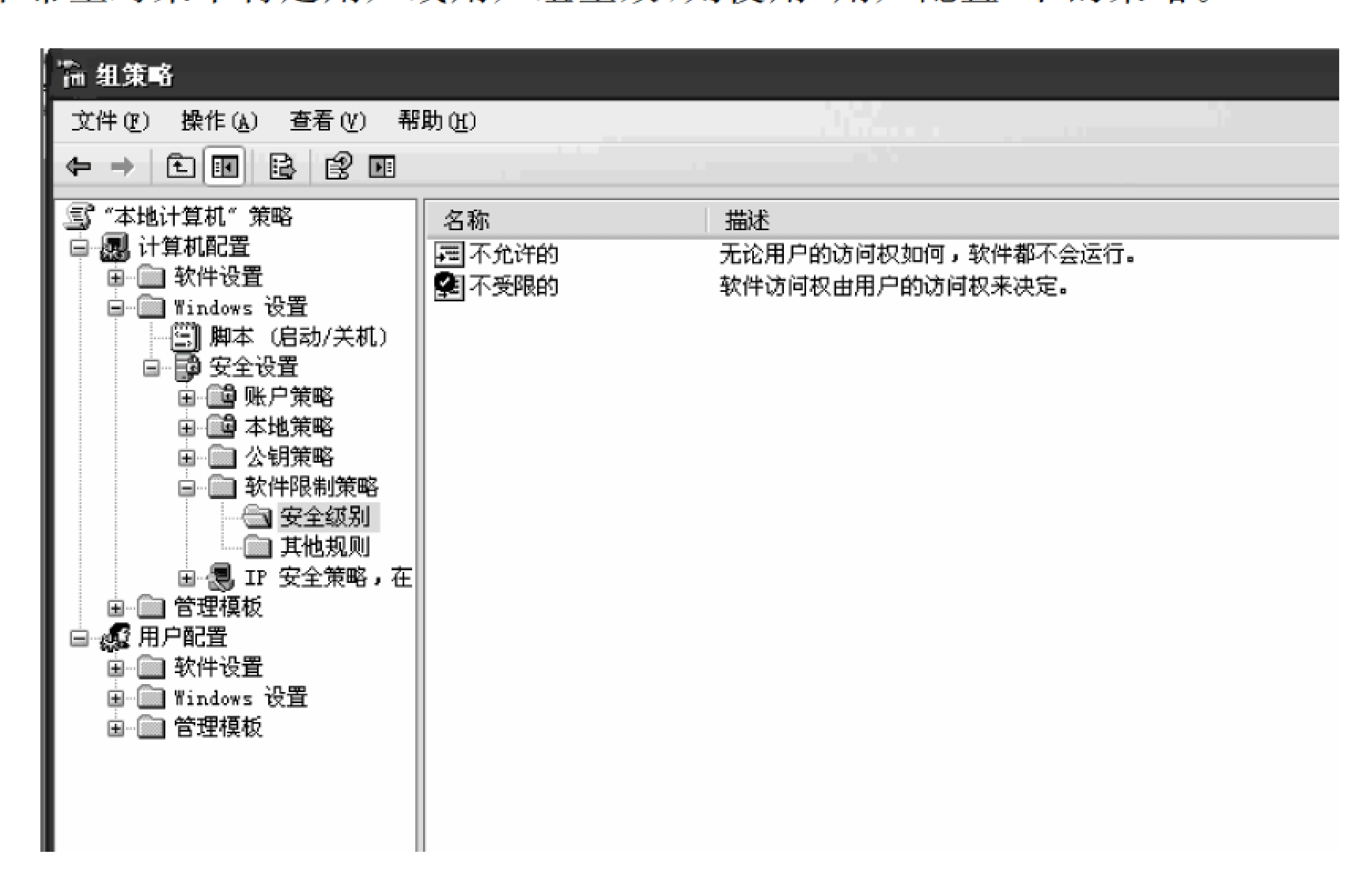


图 5.1　设置软件限制策略

在开始配置之前还需考虑一个问题，即所允许的软件都有哪些特征，所禁用的软件又有哪些特征。用户应设计出一种最佳的策略，能使所有需要的软件正确运行，所有不必要的软件都无法运行。本例中假设用户允许的大部分程序都位于系统盘(C 盘)的 Program Files 及 Windows 文件夹下，因此可以通过文件所在路径的方法决定哪些程序是被信任的。而对于安装在 D 盘的 Office 程序，可通过任意路径或文件 Hash 值的方法来决定。

软件限制规则的简单操作步骤如下：

(1) 如图 5.1 所示，单击“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”项，在“操作”菜单下选择“创建新的策略”(在 Windows XP/SP1 上，默认是没有任何策略的，但对于 Windows XP/SP2 系统，已经有了建好的默认策略)。系统将会创建“安全级别”和“其他规则”两个新条目，其中在安全级别条目下有“不允许的”和“不受限的”两条规则。前者明确默认情况下所有软件都不允许运行，只有特别配置过的少数软件才可以运行；而后者明确默认情况下所有软件都可以运行，只有特别配置过的少数软件才被禁止运行。本例中需要运行的软件都已经确定，因此需要使用“不允许的”作为默认规则。双击“不允许的”或右击后选择“属性”，然后单击“设为默认”按钮，如图 5.2 所示，并在同意警告信息后继续。



图 5.2　默认“不允许的”规则

(2) 打开“其他规则”条目，可看到默认情况下这里已经有 4 个规则，都是根据注册表路径设置的，且默认都设置为“不受限的”，如图 5.3 所示。不要修改这 4 个规则，否则系统

运行将会遇到麻烦，因为这4个路径都涉及重要系统程序及文件所在的位置。同时，位于系统盘下 Program Files 文件夹及 Windows 文件夹下的文件是允许运行的，而这4条默认规则已经包含了这些路径。

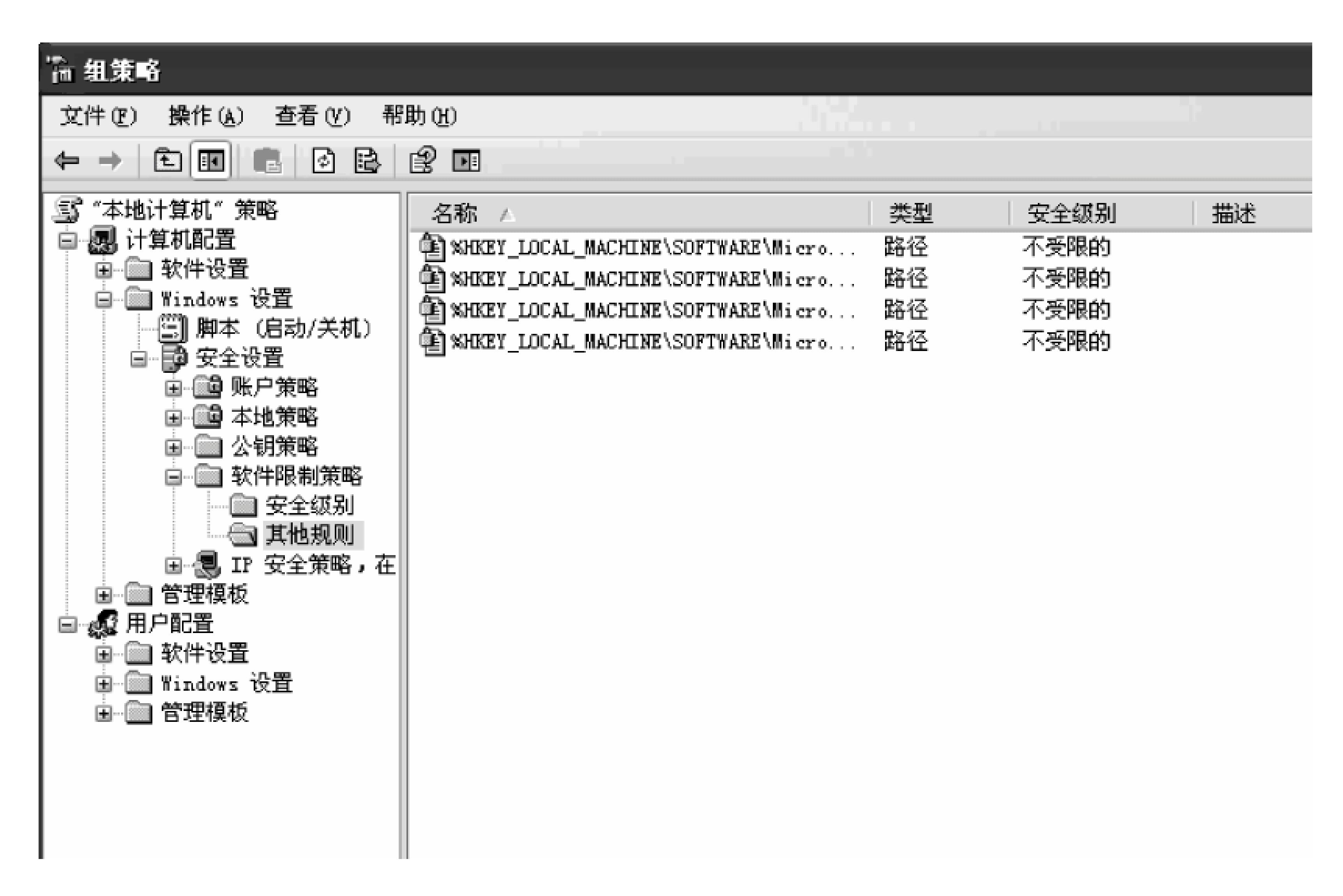


图5.3　默认的“其他规则”

(3) 右击右侧面板的空白处，选择“新散列规则”，弹出如图5.4所示的窗口。再单击“浏览”按钮，定位所有允许使用的 Office 程序的可执行文件，并双击加入。

(4) 在“安全级别”下拉菜单下双击“不受限的”选项，单击“设为默认值”→“应用”→“确定”按钮退出。这样，就完成了软件的可执行文件均为不受限的设置。

此外，根据用户的实际情况还可选择使用“强制”策略和“指派文件类型”策略。强制策略可限定软件限制策略应用到哪些文件以及是否应用到 Administrator 账户；指派文件类型策略可指定具有哪些扩展名的文件可以被系统认为是可执行文件，可以添加或删除某种类型扩展名的文件。



图5.4　添加一个规则

当软件显示策略设置好后，一旦被限制的用户试图运行被禁止的程序，那么系统将会立刻发出警告并拒绝执行。

5.1.2　TCP/IP 协议的安全性

TCP/IP 是异构网络互连的通信协议，通过它可实现各种异构网络或异种机之间的互

连通信。TCP/IP 已成为当今计算机网络最成熟、应用最广的互连协议。Internet 采用的就是 TCP/IP 协议,该协议也可用于任何其他网络,如局域网,以支持异种机的连网或异构型网络的互连。网络上各种各样的计算机上只要安装了 TCP/IP 协议,它们之间就能相互通信。运行 TCP/IP 协议的网络是一种采用包(分组)交换的网络。

TCP/IP 协议是由 100 多个协议组成的协议集,TCP 和 IP 是其中两个最重要的协议。TCP 和 IP 两个协议分别属于传输层和网络层,在 Internet 中起着不同的作用。

1. TCP/IP 协议的层次结构及主要协议

基于 TCP/IP 协议的网络体系结构比 OSI 参考模型结构更简单。TCP/IP 协议可分为 4 层,分别是网络接口层、网络层(IP)、传输层(TCP)和应用层,如图 5.5 所示。

TCP/IP	OSI
应用层	应用层 表示层 会话层
传输层(TCP)	传输层
网络层(IP)	网络层
网络接口层	数据链路层

图 5.5 TCP/IP 结构与 OSI 结构

网络接口层负责接收 IP 数据报,并把这些数据报发送到指定网络中。它与 OSI 模型中的数据链路层和物理层相对应。

网络层要解决主机到主机的通信问题,该层的主要协议有 IP 和 ICMP。IP 协议是 Internet 中的基础协议,它提供了不可靠的、尽最大努力的、无连接的数据报传递服务。ICMP 是一种面向连接的协议,用于传输错误报告控制信息。由于 IP 协议提供了无连接的数据报传送服务,在传送过程中若发生差错或意外情况则无法处理数据报,这就需要 ICMP 协议来向源节点报告差错情况,以便源节点对此做出相应的处理。

传输层的基本任务是提供应用程序之间的通信,这种通信通常称为端到端通信。传输层可提供端到端之间的可靠传送,确保数据到达无差错、不乱序。传输层的主要协议有 TCP 和 UDP。TCP 协议是在 IP 协议提供的服务基础上,支持面向连接的、可靠的传输服务。UDP(user data protocol)协议是直接利用 IP 协议进行 UDP 数据报的传输,因此 UDP 协议提供的是无连接、不保证数据完整到达目的地的传输服务。由于 UDP 不使用很繁琐的流控制或错误恢复机制,只充当数据报的发送者和接收者,因此,UDP 比 TCP 简单得多。

应用层为协议的最高层,在该层应用程序与协议相互配合,发送或接收数据。TCP/IP 协议集在应用层上有远程登录协议(Telnet)、文件传输协议(FTP)、电子邮件协议(SMTP)、域名系统(DNS)等,它们构成了 TCP/IP 的基本应用程序。

2. TCP/IP 协议安全性分析

TCP/IP 协议本身也存在着一些安全性问题,是黑客实施网络攻击的重点目标。TCP/IP 协议是建立在可信环境下的,这种基于地址的协议本身就存在泄露口令,经常会运行一些无关程序等缺陷。互联网技术屏蔽了底层网络硬件细节,使得异种网络之间可以互相通信。这就给黑客攻击网络以可乘之机。由于大量重要的应用程序都以 TCP 作为它们的传输层协议,因此 TCP 的安全性问题会对网络带来很大影响。

(1) TCP 协议

TCP 使用三次握手机制建立一条连接。攻击者可利用这三次握手过程建立有利于自

己的连接(破坏原连接),若他们再趁机插入有害数据包,则后果更严重。

TCP 协议把通过连接而传输的数据看成是字节流,用一个 32 位整数对传送的字节编号。初始序列号(ISN)在 TCP 握手时产生,产生机制与协议实现有关。攻击者只要向目标主机发送一个连接请求,即可获得上次连接的 ISN,再通过多次测量来回传输路径,得到进攻主机到目标主机之间数据包传送的来回时间(RTT)。已知上次连接的 ISN 和 RTT,很容易就能预测下一次连接的 ISN。若攻击者假冒信任主机向目标主机发出 TCP 连接,并预测到目标主机的 TCP 序列号,攻击者就能伪造有害数据包,使之被目标主机接受。

(2) IP 协议和 ICMP 协议

IP 协议提供无连接的数据包传输机制,其主要功能有寻址、路由选择、分段和组装。传输层把报文分成若干个数据包,每个包在网关中进行路由选择,穿越一个个物理网络从源主机到达目标主机。在传输过程中每个数据包可能被分成若干小段,以满足物理网络中最大传输单元长度的要求,每一小段都作为一个独立的数据包被传输,其中只有第一个数据包含有 TCP 层的端口信息。在包过滤防火墙中根据数据包的端口号检查是否合法,这样后续数据包就可以不经检查而直接通过。攻击者若发送一系列有意设置的数据包,以非法端口号为数据的后续数据包覆盖前面的具有合法端口号的数据包,那么该路由器防火墙上的过滤规则被旁路,从而攻击者便达到了进攻目的。

IPv6 设计的两种安全机制被加进了 IPv4,其中一种称为 AH(authentication header)机制,提供验证和完整性服务,但不提供保密服务;另一种称为 ESP(encapsulation security payload)机制,提供完整性服务、验证服务及保密服务。

ICMP 是在网络层中与 IP 一起使用的协议。如果一个网关不为 IP 分组选择路由、不能递交 IP 分组或测试到某种不正常状态,如网络拥挤影响 IP 分组的传递,那么就需要 ICMP 来通知源端主机采取措施,避免或纠正这些问题。ICMP 被认为是 IP 协议不可缺少的组成部分,是 IP 协议正常工作的辅助协议。

ICMP 协议存在的安全问题有:攻击者可利用 ICMP 重定向报文破坏路由,并以此增强其窃听能力;攻击者可利用不可达报文对某用户节点发起拒绝服务攻击。

3. TCP/IP 层次安全

TCP/IP 的层次不同提供的安全性也不同。例如,在网络层提供虚拟专用网络(VPN),在传输层提供安全套接层(SSL)服务等。

(1) 网络接口层安全

网络接口层与 OSI 模型中的数据链路层和物理层相对应。物理层安全主要是保护物理线路的安全,如保护物理线路不被损坏、防止线路的搭线窃听、减少或避免对物理线路的干扰等。数据链路层安全主要是保证链路上传输的信息不出现差错,保护数据传输通路畅通,保护链路数据帧不被截收等。

网络接口层安全一般可以达到点对点间较强的身份验证、保密性和连续的信道认证,在大多数情况下也可以保证数据流的安全。有些安全服务可以提供数据的完整性或至少具有防止欺骗的能力。

(2) 网络层的安全

网络层安全主要是基于以下几点考虑。

① 控制不同的访问者对网络和设备的访问。

② 划分并隔离不同安全域。

③ 防止内部访问者对无权访问区域的访问和误操作。

IP分组是一种面向协议的无连接的数据包,不同于WAN中使用的其他技术,因此要对其施以安全保护。IP包是可共享的,用户间的数据在子网中要经过很多节点进行传输。从安全角度讲,网络组件对下一个邻近节点并不了解。因为每个数据包可能来自网络中的任何地方,因此如认证、访问控制等安全服务必须在每个包基础上执行。又由于IP包的长度不同,可能要考虑每个数据包以获得与安全相关的信息。

国际上有关组织已经提出了一些对网络层安全协议进行标准化的方案,如安全协议3号(SP3)就是美国国家安全局以及标准技术协会作为安全数据网络系统(SDNS)的一部分而制定的,网络层安全协议(NLSP)是由ISO为无连接网络协议(CLNP)制定的安全协议标准。事实上,这些安全协议都使用IP封装技术。IP封装技术将纯文本的包加密,封装在外层IP报头里,当这些包到达另一端时,外层的IP报头被拆开,报文被解密,然后交付给收端用户。网络层安全协议可用来在Internet上建立安全的IP通道和虚拟专用网。其本质是:纯文本的包被加密,封装在外层的IP报头里,用来对加密包进行Internet上的路由选择;到达另一端时,外层的IP报头被拆开,报文被解密,然后送到收报地点。

网络层安全性的主要优点是它的透明性,即安全服务的提供不需要对应用程序、其他通信层次和网络部件做任何改动。主要缺点是网络层一般对属于不同进程和相应条例的包不做区别。对所有去往同一地址的包,它将按照同样的加密密钥和访问控制策略来处理。

简言之,网络层非常适合提供基于主机对主机的安全服务。相应的安全协议可用来在Internet上建立安全的IP通道和VPN。

(3) 传输层的安全

由于TCP/IP协议本身很简单,没有加密、身份验证等安全特性,因此必须在传输层建立安全通信机制,为应用层提供安全保护。传输层网关在两个节点之间代为传递TCP连接并进行控制。常见的传输层安全技术有SSL、SOCKS和PCT等。

在Internet中提供安全服务的一个想法就是强化它的IPC界面。具体做法包括双端实体的认证、数据加密密钥的交换等。Netscape通信公司遵循了这个思路,制定了建立在可靠的传输服务基础上的安全套接层(SSL)协议。

与网络层安全机制相比,传输层安全机制的主要优点是提供基于进程对进程的安全服务。这一成就如果再加上应用级的安全服务,就可以再向前跨越一大步。原则上,任何TCP/IP应用,只要应用传输层安全协议,就必定要进行若干修改以增加相应的功能,并使用不同的IPC界面。传输层安全机制就是要对传输层IPC界面和应用程序两端都进行修改。另外,基于UDP的通信很难在传输层建立起安全机制。网络层安全机制的透明性使安全服务的提供不要求应用层做任何改变,这对传输层来说是做不到的。

(4) 应用层的安全

网络层/传输层的安全协议允许为主机/进程之间的数据通道增加安全属性。本质上,这意味着真正的数据通道还是建立在主机或进程之间,但却不能区分在同一通道上传输的一个具体文件的安全性要求。比如说,如果一个主机与另一个主机之间建立起一条安全的IP通道,那么所有在这条通道上传输的IP包都自动地被加密。同样,如果一个进程和另一

个进程之间通过传输层安全协议建立起一条安全的数据通道，那么两个进程间传输的所有消息就都要自动地被加密。

如果确实想要区分一个具体文件的不同安全性要求，就必须借助于应用层的安全性。提供应用层的安全服务实际上是最灵活的处理单个文件安全性的手段。例如，一个电子邮件系统可能需要对要发出信件的个别段落实施数据签名。较低层的协议提供的安全功能一般不会知道任何要发出的信件的段落结构，从而不可能知道该对哪一部分进行签名。只有应用层能够唯一提供这种安全服务。

应用层提供的安全服务，通常都是对每个应用(包括应用协议)分别进行修改和扩充，加入新的安全功能。现已实现的 TCP/IP 应用层的安全措施有：基于信用卡安全交易服务的安全电子交易(SET)协议，基于信用卡提供电子商务安全应用的安全电子付费协议(SEPP)，基于 SMTP 提供电子邮件安全服务的私用强化邮件(PEM)，基于 HTTP 协议提供 Web 安全使用的安全性超文本传输协议(SHTTP)等。

5.2　加密文件系统

5.2.1　EFS 软件

加密文件系统(encrypting file system，EFS)是 Windows 文件系统的内置文件加密工具，它以公共密钥加密为基础，使用 CryptoAPI 架构，提供一种透明的文件加密服务。Windows 2000/XP/2003 都配备了 EFS。EFS 可对存储在 NTFS 磁盘卷上的文件和文件夹执行加密操作。对于 NTFS 卷上的文件和数据，都可以直接被操作系统加密保存，这在很大程度上提高了数据的安全性。

在使用 EFS 加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的 FEK(文件加密密钥)，然后利用 FEK 和数据扩展标准 X 算法创建加密文件，并把它存储到硬盘上，同时删除未加密的源文件。随后系统利用用户的公钥加密 FEK，并把加密后的 FEK 存储在同一个加密文件中。当用户访问被加密的文件时，系统首先利用用户的私钥解密 FEK，然后利用 FEK 解密原加密文件。在首次使用 EFS 时，如果用户还没有公钥/私钥对(统称为密钥)，则会首先生成密钥，然后再加密数据。EFS 加密文件的时候，使用对该文件唯一的对称加密密钥，并使用文件拥有者 EFS 证书中的公钥对这些对称加密密钥进行加密。因为只有文件的拥有者才能使用密钥对中的私钥，所以也只有他才能解密密钥和文件。

EFS 加密系统对用户是透明的，即如果用户加密了一些数据，那么他对这些数据的访问将是完全允许的，并不会受到任何限制。如果用户持有一个已加密 NTFS 文件的私钥，那么他就能够打开这个文件，并透明地将该文件作为普通文档使用。而其他非授权用户试图访问加密过的数据时，就会收到“访问拒绝”的提示。这说明非授权用户无法访问经过 EFS 加密后的文件。即使是有权访问计算机及其文件系统的用户，也无法读取这些加密数据。

当使用 EFS 对 NTFS 文件系统的文件或文件夹进行安全处理时，操作系统将使用 CryptoAPI 所提供的公钥和对称密钥加密算法对文件或文件夹进行加密。EFS 作为操作系统级的安全服务，内部实现机制非常复杂，但管理员和用户使用起来却非常简单。EFS

加密的用户验证过程是在登录 Windows 时进行的，只要登录到 Windows，就可以打开任何一个被授权的加密文件，而并不像第三方加密软件那样在每次存取时都要求输入密码。

当保存文件时 EFS 将自动对文件进行加密，当用户重新打开文件时系统将对文件进行自动解密。除加密文件的用户和具有 EFS 文件恢复证书的管理员之外，没有人可以读写经过加密处理的文件或文件夹。因为加密机制建立在文件系统内部，它对用户的操作是透明的，而对攻击者来说却是加密的。

如果把未加密的文件复制到经过加密的文件夹中，那么这些文件将会被自动加密。若想将加密文件移出来，如果移动到 NTFS 分区上，文件依旧保持加密属性。

在 Windows 系统中，每一个用户都有一个 SID（安全标识符）以区分各自的身份，每个人的 SID 都不相同且是唯一的（SID 可类似人的指纹）。因为理论上没有 SID 相同的用户，因而用户的密钥也就绝不会相同。在第一次加密数据时，操作系统就会根据加密者的 SID 生成该用户的密钥，并把公钥和私钥分开保存起来，供用户加密和解密数据。这一切可保证 EFS 机制的可靠性。

在某些情况下会发生诸如用户私钥丢失或雇员离开公司等突发事件时，EFS 提供了一种恢复代理机制，可以恢复经 EFS 加密的文件信息。当使用 EFS 时，系统将自动创建一个独立的恢复密钥对，并存储在管理员 EFS 文件恢复证书中。恢复密钥对的公钥用于加密原始的加密密钥，并在紧急情况下使用私钥来恢复加密文件的密钥，从而恢复经过加密的文件。Windows 2000 系统在单机和工作组环境下，默认的恢复代理是 Administrator；Windows XP 系统在单机和工作组环境下没有默认的恢复代理；而在域环境中所有加入域的 Windows 2000/XP 计算机，默认的恢复代理全部是域管理员。这一切又可保证被加密数据的安全性。

使用 EFS 加密功能要保证两个条件，第一要保证操作系统是 Windows 2000/XP/2003，第二要保证文件所在的分区格式是 NTFS 格式（FAT32 分区里的数据是无法加密的；如果要使用 EFS 对其进行加密，就必须将 FAT32 格式转换为 NTFS）。

值得注意的是，被 EFS 加密的数据也不是绝对安全的，如果没有合适的密钥，虽然无法打开被 EFS 加密过的文件，但仍可以将其删除。所以对于重要文件，最佳的做法是综合使用 NTFS 权限和 EFS 加密两项安全措施。这样，如果非法用户没有合适的权限，将不能访问受保护的文件和文件夹，因此也就不能删除文件了；而有些用户即使拥有权限，没有密钥同样还是打不开加密数据。

NTFS 分区上保存的数据还可以被压缩，但是一个文件不能同时被压缩和加密。Windows 的系统文件和系统文件夹无法被加密。

综上所述，可概括 EFS 系统具有如下特性。

(1) 用户加密或解密文件或文件夹很方便，访问加密文件简单容易。

(2) EFS 加密系统对用户是透明的。

(3) 加密后的数据无论怎样移动都保持加密状态。

(4) EFS 加密机制和操作系统紧密结合，用户不必为加密数据安装额外软件，可节约使用成本。

(5) EFS 与 NTFS 紧密地结合在一起。

(6) 通过 EFS 加密敏感性文件，会增加更多层级的安全性防护。

5.2.2　EFS 加密和解密应用实践

1. EFS 加密和解密操作

（1）EFS 加密文件或文件夹

如要对 C 盘下的 abc 文件夹进行 EFS 加密，其操作过程如下（注意：EFS 加密只在 NTFS 文件系统上才有效）：

第 1 步：右击要加密的文件夹，选择“属性”选项，弹出如图 5.6 所示该文件夹的属性窗口。

第 2 步：在“属性”窗口中单击“高级”按钮，在弹出的“高级属性”窗口中选择“加密内容以便保护数据”选项，如图 5.7 所示，单击“确定”按钮。

第 3 步：在随后的属性窗口中单击“应用”按钮，弹出“确认属性更改”对话框，如图 5.8 所示。如选择“仅将更改应用于该文件夹”，系统将只对文件夹加密，文件夹里面已有的内容并没被加密，但是此后在文件夹中创建的文件或文件夹将被加密；如选择“将更改应用于该文件夹、子文件夹和文件”，文件夹内部的所有内容均被加密。



图 5.6　加密文件夹属性

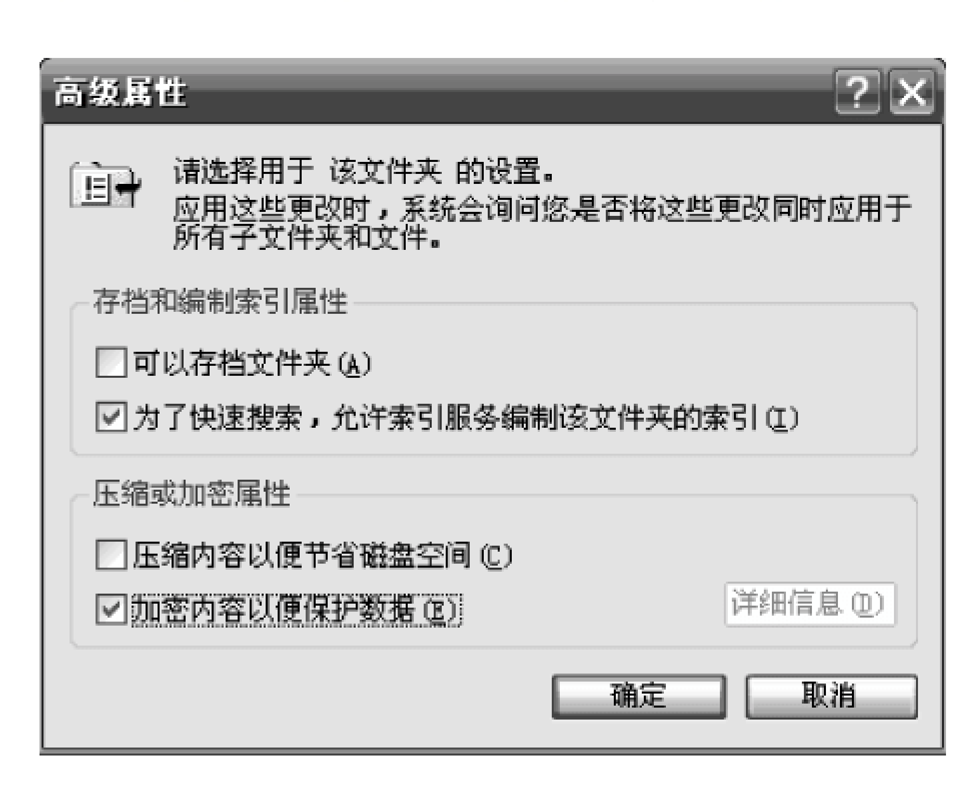


图 5.7　“高级属性”窗口

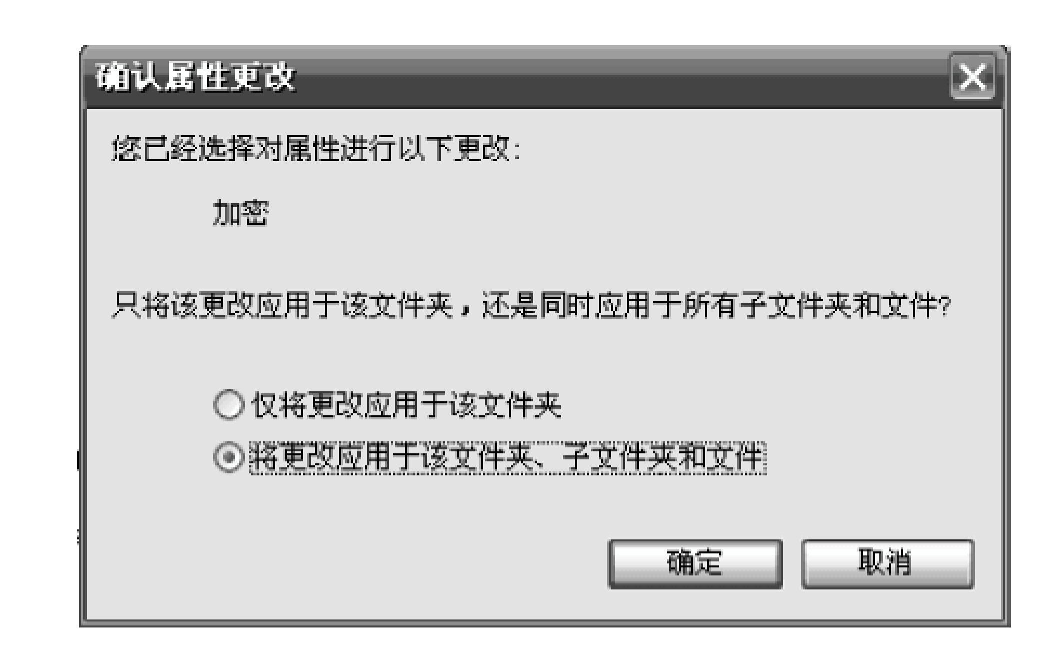


图 5.8　“确认属性更改”窗口

第 4 步：单击“确定”按钮，完成加密操作。

现在有了一个被 EFS 加密过的文件夹，以后如果用户要对某个文件或文件夹进行 EFS 加密，也可以把它们移到该文件夹中，这样这些文件或文件夹就会被自动加密。

（2）密钥备份和解密文件/文件夹

EFS 加密操作虽然简单，但是如果用户重装了系统，此后即使再利用原来的用户名和密码，也无法打开 EFS 加密过的文件或文件夹。这是因为加密时的密钥信息保存在原系统中，重装系统后原密钥信息丢失。因此用户在加密时应该及时备份密钥，这样以后即使重装系统，也可利用备份密钥打开加密文件或文件夹。

在 Windows XP 中，备份密钥的操作过程如下：

第 1 步：单击“开始”→“运行”命令，输入“certmgr. msc”并按回车键，打开证书管理器（密钥的导出和导入工作都将在这里进行）。

第 2 步：选择“当前用户” →“个人” →“证书”菜单，可以看见一个与用户名同名的证书（如果用户还没有加密任何数据，这里是不会有证书的）。假如有多份证书，可选择“预期目的”为“加密文件系统”的那份证书。

第 3 步：右击“证书”选项，选择“所有任务”→“导出”菜单，如图 5. 9 所示，于是就会弹出一个如图 5. 10 所示的“证书导出向导”窗口。



图 5. 9　选择个人证书



图 5. 10　证书导出向导

第 4 步：单击“下一步”按钮，弹出如图 5. 11 所示的导出密钥窗口，在向导中会询问用户是否导出私钥。在这里要选择“是，导出私钥” 按钮。



图 5.11　导出证书密钥

第 5 步：单击“下一步”按钮，弹出如图 5.12 所示的对话框。按照提示要求，输入和确认该用户的密码后，单击“下一步”按钮再选择想要保存的路径并单击“确定”按钮，最后私钥(文件后缀为 PFX)便成功导出，如图 5.13 所示；若在图 5.11 中选择“不，不要导出私钥”按钮，按照提示要求输入后便可导出证书(文件后缀为 CER)。



图 5.12　输入并确认密码



图 5.13　完成证书导出向导

至此，导出任务完成，如图 5.14 所示。



图 5.14 导出成功

以后利用这些备份密钥(证书和私钥)即可恢复加密数据。其他用户如果获得本用户的备份密钥，也能轻松解密其加密文件，因此一定要保管好备份密钥。

(3) 找回 EFS 加密文件

当加密文件的系统账户出现问题或重装系统后，EFS 加密文件就无法访问了。可以采用如下两种解决方法。

① 利用备份的 PFX 私钥

如果备份有 PFX 私钥文件，利用它打开加密文件很容易。操作过程如下：

第 1 步：找到备份的 PFX 私钥文件，右击该文件，并选择“安装 PFX”选项，如图 5.15 所示；系统弹出“证书导入向导”对话框，如图 5.16 所示。

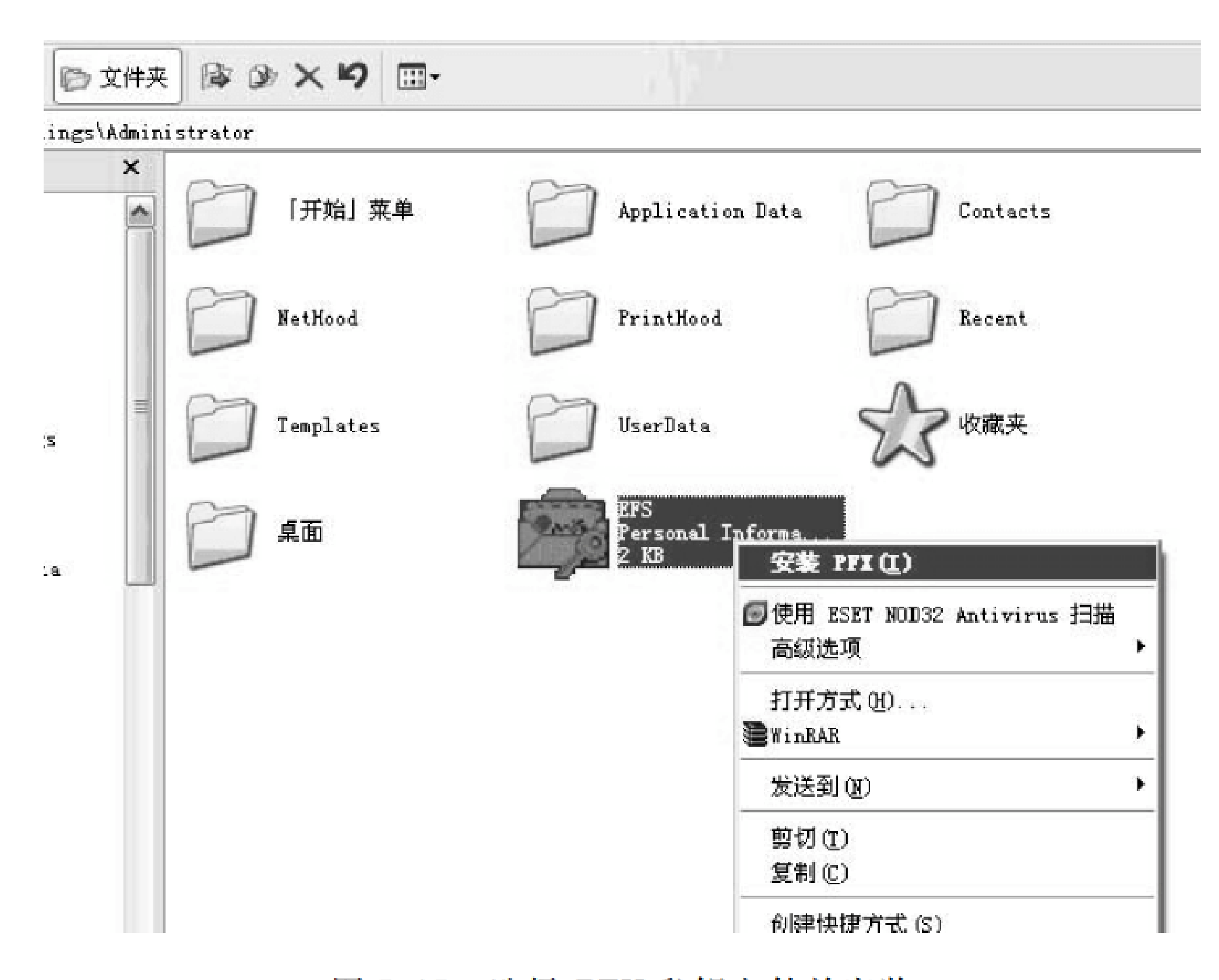


图 5.15 选择 PFX 私钥文件并安装

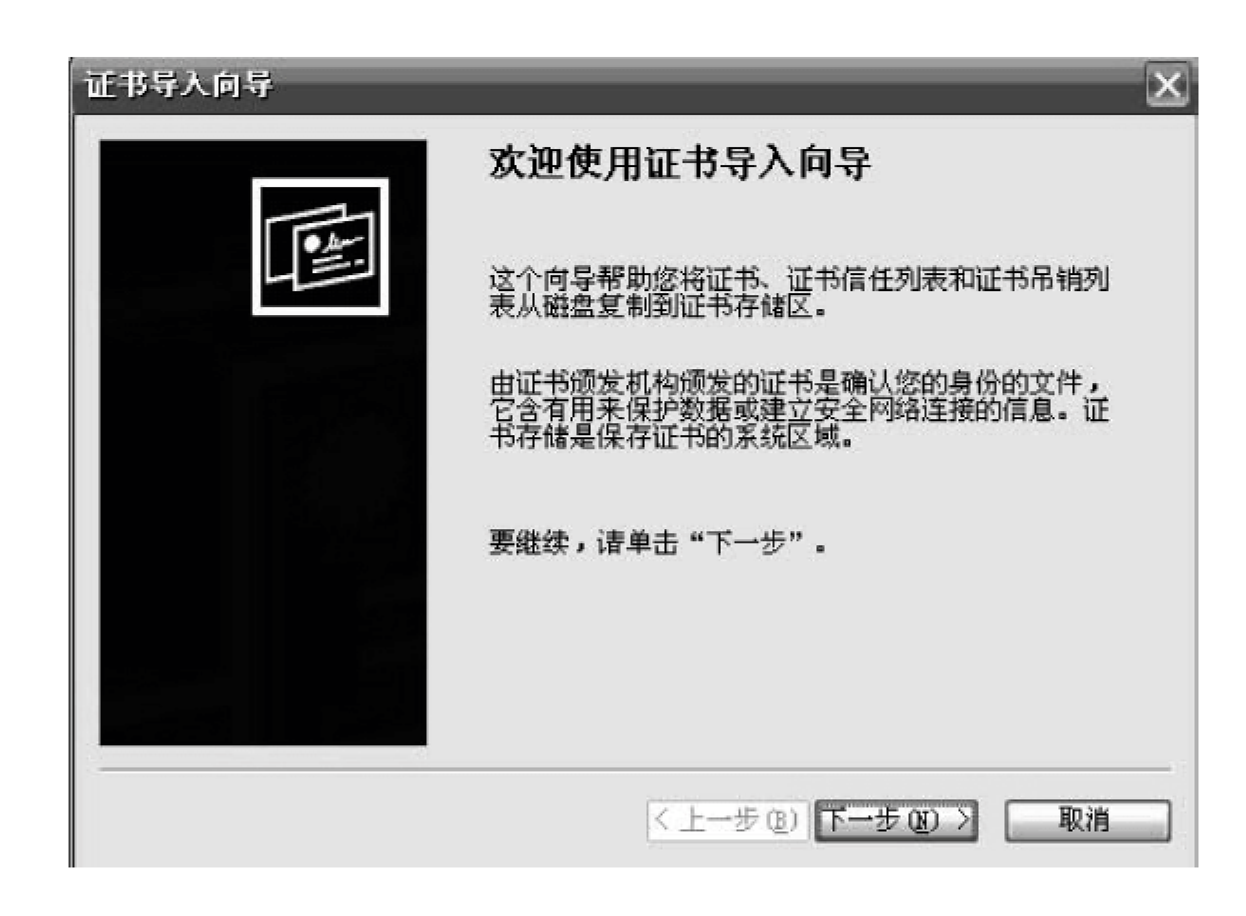


图 5.16 进入证书导入向导

第 2 步：单击“下一步”按钮，在弹出的对话框中输入要导入的文件名称，如 EFS.pfx，如图 5.17 所示。



图 5.17　输入文件名

第 3 步：单击“下一步”按钮，在弹出的对话框中再输入当初导出证书时输入的密码，如图 5.18 所示，然后选择“根据证书类型，自动选择证书存储区”选项，如图 5.19 所示。



图 5.18　输入密码

证书导入向导
证书存储
证书存储区是保存证书的系统区域。
Windows 可以自动选择证书存储区，或者您可以为证书指定一个位置。
根据证书类型，自动选择证书存储区(U)
将所有的证书放入下列存储区(P)
证书存储:
浏览(R)...
<上一步(B)
下一步(N)>
取消

图 5.19　选择证书存储区域

第 4 步：单击“下一步”按钮并在弹出的如图 5.20 所示的窗口中单击“完成”按钮，弹出导入成功提示，如图 5.21 所示。此后就可以访问 EFS 加密文件了。



图 5.20 显示导入设置



图 5.21 导入成功

② 利用备份的 CER 证书

假如用户以前未备份 PFX 私钥文件，但是备份过 CER 证书，如果又重装了系统，就没有办法打开加密文件了；假如用户还没有重装系统，则可利用备份的 CER 证书进行类似 PFX 的操作：

第 1 步：找到备份的 CER 证书文件，右击该文件，并选择“安装证书(I)”选项，如图 5.22 所示，系统将弹出“证书导入向导”对话框。



图 5.22 选择 CER 文件并安装

第 2 步：在出现的“证书导入向导”对话框中选择“将所有的证书放入下列存储区”选项，并单击“浏览”按钮，如图 5.23 所示。



图 5.23 选择存储区域

第 3 步：在出现的选择证书存储窗口中选择“个人”存储区并单击“确定”按钮，即可把证书导入到“个人”存储区，如图 5.24 所示。

第 4 步：单击“下一步”按钮，完成证书导入向导，如图 5.25 所示。



图 5.24 选择“个人”区域



图 5.25 完成证书导入向导

第 5 步：单击“完成”按钮后，即可看见完成证书导入提示，如图 5.21 所示。

第 6 步：执行“开始”→“运行”命令，输入“certmgr. msc”然后按回车键，打开证书管理器。

第 7 步：选择“当前用户”→“个人”→“证书”路径，右击“证书”所有者，选择“所有任务”→“用相同密钥续订证书”菜单，如图 5.26 所示。

此后就可以访问 EFS 加密文件了。

(4) 解密 EFS 加密的文件或文件夹

如果用户要对已被 EFS 加密过的文件或文件夹解密，或是想取消已对某个文件或文件夹进行的 EFS 加密，则可采取如下操作过程。

第 1 步：打开 Windows 资源管理器，右击已加密的文件或文件夹，单击“属性”选项。



图 5.26　续订个人证书

第 2 步：在“常规”选项卡上单击“高级”按钮；在弹出的如图 5.7 所示的窗口中取消“加密内容以便保护数据”复选框前面的“√”。

第 3 步：确定后在出现的“确认属性更改”窗口中就显示对属性的更改为“解密”，如图 5.27 所示(可与图 5.8 比较)，最后单击“确定”按钮即可。



图 5.27　确认属性更改

2. EFS 的其他操作

EFS 系统除了具有对文件或文件夹的加密/解密功能外，还有如下一些常用操作：

(1) 禁用 EFS 加密功能

如果用户不喜欢 EFS 功能，可以彻底禁用它。执行“开始”→“运行”命令，输入“regedit”并按回车键，打开注册表编辑器，依次展开到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS，然后新建一个 Dword 值 EfsConfiguration，并将其键值设为 1。这样本机的 EFS 加密功能就被彻底禁用了。

(2) 将 EFS 选项添加至快捷菜单

如果想将 EFS 选项添加至快捷菜单，其操作过程为：执行“开始”→“运行”命令，输入“regedit” 并按回车键，打开注册表编辑器，依次展开到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced，然后新建一个 Dword 值 EncryptionContextMenu，并将它的键值设为 1。

注意：*为确保对注册表进行修改，应在自己的计算机上拥有管理员账号。这样当用户右击某一存储于 NTFS 磁盘卷上的文件或文件夹时，加密或解密选项便会出现在随后弹出的快捷菜单上。*

(3) 不加密文件夹下的子文件夹

在利用 EFS 加密的过程中用户常会遇到这种情况：用户需要加密某一个文件夹，此文件夹下还有很多子文件夹，而用户有时不想加密位于此文件夹下的某一个或几个子文件夹，

这样，可用如下两种方法之一解决：

① 将不需要加密的子文件夹剪切移出，单独设立文件夹，脱离与原文件夹的关系，然后再加密原文件夹。这也是很多用户常用的方法。这样做的缺点是破坏了原来的目录结构，加密和保持原有的目录结构产生了矛盾。

② 在不需要加密的子文件夹下建立一个名为 Desktop.ini 的文件，打开该文件并输入以下内容：

```
[encryption]
Disable = 1
```

输入完毕保存并关闭该文件。这样，以后如要加密其父文件夹，当加密到该子文件夹时就会遇到错误的信息提示，单击“忽略”按钮后即可跳过对该子文件夹的加密，而其父文件夹的加密不会受到影响。

(4) 在命令提示符下加密/解密文件

如果用户不喜欢在图形界面操作，还可以在命令提示符下用 cipher 命令完成对文件和文件夹的加密/解密操作。其命令格式为：

```
cipher [/e /d] 文件夹或文件名 [参数]
```

如要为 C 盘根目录下的 abc 文件夹加密，就输入“cipher /e c:\abc”，按回车键后即可完成对该文件夹的加密。如要对该文件夹进行解密，则输入“cipher /d c:\abc”，按回车键后即可完成对该文件夹的解密。/e 是加密参数，/d 是解密参数，其他更多的参数和用法请在命令提示符后输入“cipher /?”查询即可得到。

5.3 Kerberos 系统

Kerberos 是一种提供网络认证服务的系统，其设计目标是通过密钥系统为 Client/Server 应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无须基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。

5.3.1 Kerberos 概述

Kerberos 是为 TCP/IP 网络系统设计的一种基于对称密钥密码体制的第三方认证协议。Kerberos 认证协议在许多系统中都获得广泛应用，如 Kerberos v5 是微软公司 Windows 2000/XP/2003 等操作系统的基础认证协议。Windows 2000/2003 默认模式中的模式域就使用了 Kerberos。

Kerberos 在 Windows 2003 中的执行完全符合 IETF 的 Kerberos v5 规范，该规范得到了广泛的支持，这意味着 Windows 2003 域(也称为 Kerberos 领域)发出的票证可以在其他领域中使用，如运行 MacOS、NetWare、UNIX、AIX、IRIX 等系统的网络。

Kerberos 认证协议定义了客户端和密钥分配中心(Key Distribution Center，KDC)的认证服务之间的安全交互过程。KDC 由认证服务器 AS 和票证授权服务器 TGS 两部分组

成。Kerberos 协议根据 KDC 的第三方服务中心来验证网络中计算机的身份,并建立密钥以保证计算机间安全连接。Kerberos 允许一台计算机通过交换加密消息在整个非安全网络上与另一台计算机互相证明身份。一旦身份得到验证,Kerberos 协议将会给这两台计算机提供密钥,以进行安全通信对话。Kerberos 协议可以认证试图登录上网用户的身份,并通过使用密钥密码为用户间的通信加密。

Kerberos 以票证(ticket)系统为基础,票证是 KDC 发出的一些加密数据包,它可标识用户的身份及其网络访问权限。每个 KDC 负责一个领域(realm)的票证发放。KDC 类似于发卡机构,"票证"类似通行"护照",它带有安全信息。在 Windows 2003 中,每个域也是一个 Kerberos 领域,每个 Active Directory 域控制器(DC)就是一个 KDC。执行基于 Kerberos 的事务时,用户将透明地向 KDC 发送票证请求。KDC 将访问数据库以验证用户的身份,然后返回授予用户访问其他计算机的权限的票证。

Windows 系统中采用多种措施提供对 Kerberos 协议的支持,在系统的每个域控制器中都应用了 KDC 认证服务。Windows 系统中应用了 Kerberos 协议的扩展,除共享密钥外,还支持基于公开密钥密码的身份认证机制。Kerberos 公钥认证的扩展允许客户端在请求一个初始 TGT(TGT 称为票据授权票证,是一个 KDC 发给验证用户的资格证)时使用私钥,而 KDC 则使用公钥来验证请求,该公钥是从存储在活动目录中用户对象的 X.509 证书中获取的。用户的证书可以由权威的第三方发放,也可以由 Windows 系统中的微软证书服务器产生。初始认证以后,就可以使用标准的 Kerberos 来获取会话票证,并连接到相应的网络服务。

5.3.2 Kerberos 应用及设置

1. Kerberos 的应用

Kerberos 允许网络上的通信实体互相证明彼此的身份,并且能够阻止窃听和重放等攻击。此外,它还能够提供对通信数据保密性和完整性的保护。

当用户初始登录 Windows 时,Kerberos 安全服务提供者(security support provider, SSP)利用基于用户口令的加密散列获取一个初始 Kerberos 票证 TGT。Windows 系统把 TGT 存储在与用户登录上下文相关的工作站的票证缓存中。当客户端想要使用网络服务时,Kerberos 首先检查票证缓存中是否有该服务器的有效会话票证。如果没有,则向 KDC 发送 TGT 请求一个会话票证,以便服务器提供服务。请求的会话票证也存储在票证缓存中,以用于后续对同一个服务器的连接,直到票证超期为止。如果在会话过程中票证超期, Kerberos SSP 将返回一个响应的错误值,允许客户端和服务器刷新票证,产生一个新的会话密钥,并恢复连接。在初始连接消息中,Kerberos 把会话票证提交给远程服务,会话票证中的一部分使用了服务和 KDC 共享的密钥进行加密。因为服务器端的 Kerberos 有服务器密钥的缓存复制,所以,服务器不需要到 KDC 进行认证,而直接可以通过验证会话票证来认证客户端。在服务器端,采用 Kerberos 认证系统的会话建立速度要比 NTLM 认证快得多。因为使用 NTLM 在服务器获取用户的信任书后,还要与域控制器建立连接,对用户进行重新认证。

在 Windows 2003 域中,KDC 通常安装在 Active Directory 服务器上。它们不会按照

应用程序进程进行连接,而是作为单独的服务进程运行。但由于 KDC 总是安装在 DC 上,所以可通过查找 DC 的主机地址来解析 KDC 域名,也可将 Windows 2003 服务器安装在非 Windows 2003 域中,这时 Windows 2003 服务器仍然能够进行 Kerberos 验证,但要保证其域名能被正确地解析成对应主机地址。

Kerberos 验证分为初始验证和后续验证两个阶段。

(1) 初始验证

客户机(用户或 NFS 服务)通过从 KDC 请求 TGT 开始 Kerberos 会话。此请求通常在登录时自动完成。TGT 可标识用户的身份并允许用户获取多个“签证”,此处的“签证”(票证)是用于远程计算机或网络服务。TGT 与其他各种票证一样也具有有限的生命周期,区别在于基于 Kerberos 的命令会通知用户拥有护照并为用户取得签证,而用户不必亲自执行该事务。

KDC 可创建 TGT,并采用加密形式将其发送回客户机,客户机使用其口令来解密 TGT;客户机在拥有有效的 TGT 后,只要该 TGT 未到期,便可以请求所有类型网络操作(如 rlogin 或 telnet)的票证。每次客户机执行唯一的网络操作时,都将从 KDC 请求该操作的票证。

(2) 后续验证

首先,客户机通过向 KDC 发送其 TGT 作为其身份证明,从 KDC 请求特定服务(如远程登录到另一台计算机)的票证;然后 KDC 将该特定服务的票证发送到客户机;最后客户机将票证发送到服务器。使用 NFS 服务时,NFS 客户机会自动透明地将 NFS 服务的票证发送到 NFS 服务器。

Kerberos 的认证过程如下:

① 客户机向认证服务器(AS)发送请求,要求得到某服务器的证书。

② AS 的响应包含这些用客户端密钥加密的证书(证书主要由服务器 ticket 和一个临时加密密钥——会话密钥构成)。

③ 客户机将 ticket(包括由服务器密钥加密的客户机身份和一份会话密钥的复制件)传送到服务器上。

会话密钥可用来认证客户机或认证服务器,也可用来为通信双方以后的通信提供加密服务,或通过交换独立子会话密钥为通信双方提供进一步的通信加密服务。

2. Kerberos 的安装设置

Kerberos 可用来为网络上的各种 Server 提供认证服务,使得口令不再是以明文方式在网络上传输。这里介绍在 Linux RedHat 8.0 环境下使用 Kerberos 自己提供的 Ktelnetd、Krlogind 和 Krshd 替代传统的 telnetd、rlogind 和 rshd 服务。

Kerberos 安装的硬件环境为一台 i386 机器,安装软件包为 krb5-server-1.2.5-6、krb5-workstation-1.2.5-6 和 krb5-libs-1.2.5-6。

```
rpm - ivhkrb5 - libs - 1.2.5 - 6.i386.rpm
rpm - ivhkrb5 - server - 1.2.5 - 6.i386.rpm
rpm - ivhkrb5 - workstation - 1.2.5 - 6.i386.rpm
```

上述要求满足后,就可以先配置 KDC 服务器,然后配置 Ktelnetd、Krlogind 和 Krshd

服务器，最后可以使用 krb5-workstation 提供的 telnet、rlogin 和 rsh 来登录这些服务。安装步骤如下：

（1）生成 Kerberos 的本地数据库

```
kdb5_utilcreate - rEXAMPLE.COM - s
```

该命令用来生成 Kerberos 的本地数据库，包括 principal、principal. OK 和 principal. kadm5 文件；principal. kadm5. lock. -r 指定 realm，例如 EXAMPLE. COM。

（2）生成账号

Kerberos 用 principal 来表示 realm 下的一个账户，表示为 primary/instance@realm。例如，username/80. 191. 89. 92@EXAMPLE. COM，这里假设 80. 191. 89. 92 是客户机的 IP 地址。

在数据库中加入管理员账户：

```
/usr/Kerberos/sbin/kadmin.local
     kadmin.local:addprincadmin/admin@EXAMPLE.COM
```

在数据库中加入用户的账号：

```
kadmin.local:addprincusername/80.191.89.92@EXAMPLE.COM
```

在数据库中加入 Ktelnetd、Krlogind 和 Krshd 公用的账号：

```
kadmin.local:addprinc - randkeyhost/80.191.89.92@EXAMPLE.COM
```

（3）检查

检查/var/Kerberos/krb5kdc/kadm5. keytab 是否有如下语句：

```
* /admin@EXAMPLE.COM *
```

如果没有，添加上即可。

（4）修改/etc/krb5. conf 文件

修改所有的 realm 为 EXAMPLE. COM，并且加入下列句子：

```
kdc = 80.191.89.92:88
admin_server = 80.191.89.92:749
```

（5）在/etc/krb. conf 中加入语句

在/etc/krb. conf 中加入下列语句：

```
EXAMPLE.COM
EXAMPLE.COM80.191.89.92:88
EXAMPLE.COM80.191.89.92:749adminserver
```

（6）启动 kdc 服务器和 Ktelnetd、Krlogind、Krshd

```
/etc/init.d/krb5kdcrestart
     Chkconfigkloginon
     Chkconfigkshellon
     Chkconfigekloginon
     chkconfigkrb5 - telneton
```

```
/etc/init.d/xinetdrestart
```

(7) 制作本地缓存

将 username/80.191.89.92@EXAMPLE.COM 的 credentials 取到本地作为 cache，这样以后就可以不用重复输入 password 了。

```
kinitusername/80.191.89.92
```

如果顺利，在/tmp 下会生成文件 krb5 *。这一步如果不通，那么就必须检查以上步骤是否有错。可以用 klist 命令查看 credential。

(8) 导出用户密钥

eXPorthost/80.191.89.92@EXAMPLE.COM 的 key 到/etc/krb5.keytab，Ktelnetd、Krlogind 和 Krshd 需要/etc/krb5.keytab 来验证 username/80.191.89.92 的身份。

```
kadmin.local:ktadd - k/etc/krb5.keytabhost/80.191.89.92
```

(9) 修改～/.k5login 文件

在其中加入 username/80.191.89.92@EXAMPLE.COM，表示允许 username/80.191.89.92@EXAMPLE.COM 登录该账户。

```
catusername/80.191.89.92@EXAMPLE.COM >>～/.k5login
```

(10) 测试 Kerberos 客户端

```
krsh80.191.89.92 - kEXAMPLE.COM
krlogin80.191.89.92 - kEXAMPLE.COM
rlogin80.191.89.92 - kEXAMPLE.COM
rsh80.191.89.92 - kEXAMPLE.COM
telnet - x80.191.89.92 - kEXAMPLE.COM
```

5.4 IPSec 系统

5.4.1 IPSec 概述

IP 安全协议(IP Security，IPSec)是网络安全协议的一个工业标准，也是目前 TCP/IP 网络的安全化协议标准。IPSec 最主要的功能是为 IP 通信提供加密和认证，为 IP 网络通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，有效抵御网络攻击，同时保持其易用性。

IPSec 的目标是为 IP 提供互操作高质量的基于密码学的一整套安全服务，其中包括访问控制、无连接完整性、数据源验证、抗重放攻击、机密性和有限的流量保密。这些服务都在 IP 层提供，可以为 IP 和其上层协议提供保护。

IPSec 不是一个单独的协议，它由一系列协议组成，包括网络认证协议(AH 也称认证报头)、封装安全载荷协议(ESP)、密钥管理协议(IKE)和用于网络认证及加密的一些算法等。其中 AH 协议定义了认证的应用方法，提供数据源认证和完整性保证；ESP 协议定义了加密和可选认证的应用方法，提供可靠性保证。在实际进行 IP 通信时，可以根据实际安

全需求同时使用这两种协议或选择使用其中的一种。AH 和 ESP 都可以提供认证服务，不过，AH 提供的认证服务要强于 ESP。IPSec 规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换，向上层提供访问控制、数据源认证、数据加密等网络安全服务。IPSec 可应用于虚拟专用网络（VPN）、应用级安全以及路由安全三个不同的领域，但目前主要用于 VPN。

IPSec 既可以作为一个完整的 VPN 方案，也可以与其他协议配合使用，如 PPTP、L2TP。它工作在 IP 层（网络层），为 IP 层提供安全性，并可为上一层应用提供一个安全的网络连接，提供基于一种端-端的安全模式。由于所有支持 TCP/IP 协议的主机进行通信时，都要经过 IP 层的处理，所以提供了 IP 层的安全性就相当于为整个网络提供了安全通信的基础。鉴于 IPv4 的应用仍然很广泛，所以后来在 IPSec 的制定中将 IPv6 中的安全支持也增添进了 IPv4。

IPSec 可用于 IPv4 和 IPv6 环境。它有两种工作模式：一种是隧道模式；另一种是传输模式。在隧道模式中，整个 IP 数据包被加密或认证，成为一个新的更大的 IP 包的数据部分，该 IP 包有新的 IP 报头，还增加了 IPSec 报头。在传输模式中，只对 IP 数据包的有效负载进行加密或认证，此时继续使用原始 IP 头部。隧道模式主要用在网关和代理上，IPSec 服务由中间系统实现，端节点并不知道使用了 IPSec。在传输模式中，两个端节点必须都实现 IPSec，而中间系统不对数据包进行任何 IPSec 处理。

通信双方如果要用 IPSec 建立一条安全的传输通道，需要事先协商好将要采用的安全策略，包括加密机制和完整性验证机制及其使用的算法、密钥、生成期限等。一旦发收双方协商好使用的安全策略，可以说双方（两台计算机）之间建立了一个安全关联（Securlty Association，SA）。

IETF 已经建立了一个安全关联和密钥交换方案的标准方法，它将 Internet 安全关联和密钥管理协议（ISAKMP）以及 Oakley 密钥生成协议进行了合并。ISAKMP 集中了安全关联管理，减少了连接时间。Oakley 生成并管理用来保护信息的身份验证密钥。为保证通信的成功和安全，ISAKMP/Oakley 执行密钥交换和数据保护两个阶段的操作。通过使用在两台计算机上协商，从而达成一致的加密和身份验证算法保证机密性和身份验证。

5.4.2 IPSec 中加密与完整性验证机制

IPSec 可对数据进行加密和完整性验证。其中，AH 协议只能用于对数据报头进行完整性验证，而 ESP 协议可用于对数据的加密和完整性验证。

IPSec 的认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭篡改。IPSec 的加密机制通过对数据进行编码来保证数据的机密性，以防数据在传输过程中被窃听。为了进行加密和认证，IPSec 还需要有密钥的管理和交换功能，以便为加密和认证提供所需要的密钥并对密钥的使用进行管理。以上三方面的工作分别由 AH、ESP 和 IKE 三个协议规定。

1. 安全关联（SA）

IPSec 中一个重要概念就是 SA，所谓安全关联是指安全服务与它服务的载体之间的一个“连接”，即是能为双方之间的数据传输提供某种 IPSec 安全保障的一个简单连接。SA 可

以看成是两个 IPSec 对等端之间的一条安全隧道。SA 是策略和密钥的结合,它定义用来保护端-端通信的常规安全服务、机制和密钥。SA 可由 AH 或 ESP 提供,当给定了一个 SA,就确定了 IPSec 要执行的处理。

在 SA 中,两台计算机在如何交换和保护信息方面达成一致。可为不同类型的流量创建独立的 SA,例如,当一台计算机与多台计算机同时进行安全通信时可能存在多种关联。这种情况经常发生在当计算机作为文件服务器或向多个客户提供服务的远程访问服务器的时候。一台计算机也可以与另一台计算机有多个 SA,例如在两台主机之间为 TCP 建立独立的 SA,并在同样两台机器之间建立另一条支持 UDP 的 SA,甚至可以为每个 TCP 或 UDP 端口建立分离的 SA。

2. 认证协议(AH)

IPSec 认证协议(AH)为整个数据包提供身份认证、数据完整性验证和抗重放服务。AH 通过一个只有密钥持有人才知道的"数字签名"来对用户进行认证。这个签名是数据包通过特别的算法得出的独特结果。AH 还能维持数据的完整性,因为在传输过程中无论多小的变化被加载,数据包头的数字签名都能把它检测出来。由于 AH 不能加密数据包所加载的内容,因而它不保证任何的机密性。两个最常用的 AH 标准是 MD5 和 SHA-1,MD5 使用最多达 128 位的密钥,而 SHA-1 通过最多达 160 位密钥提供更强的保护。重放攻击是通过采用单调递增序列号来预防的。序列号不允许循环使用,因此,当计数器达到其最大值时,不能恢复到 0。IPSec 要求在计数器达到上限时,必须建立一个新的安全关联,新的安全关联有新的计数器和加密密钥。

AH 协议为 IP 通信提供数据源认证和数据完整性验证,它能保护通信免受篡改,但并不加密传输内容,不能防止窃听。AH 联合数据完整性保护并在发送接收端使用共享密钥来保证身份的真实性;使用 Hash 算法在每一个数据包上添加一个身份验证报头来实现数据完整性验证。验证过程中需要预约好收发两端的 Hash 算法和共享密钥。

AH 可与很多各不相同的算法一起工作。AH 要校验源地址和目的地址这些标明发送设备的字段是否在路由过程中被改变过。如果校验没通过,分组就会被抛弃。通过这种方式,AH 就为数据的完整性和原始性提供了鉴定。

为了建立 IPSec 通信,两台主机在 SA 协定之前必须互相认证,有如下 3 种认证方法。

(1) Kerberos 方法

Kerberos v5 常用于 Windows 2003,是其默认认证方式。Kerberos 能在域内进行安全协议认证,使用时,它既对用户的身份也对网络服务进行验证。Kerberos 的优点是可以在用户和服务器之间相互认证,也具有互操作性。Kerberos 可以在 Server 2003 域和使用 Kerberos 认证的 UNIX 环境系统之间提供认证服务。

(2) 公钥证书(PKI)方法

PKI 用来对非受信域的成员、非 Windows 客户或没有运行 Kerberos v5 认证协议的计算机进行认证,认证证书由一个作为证书机关的系统签署。

(3) 预先共享密钥方法

在预先共享密钥认证中,计算机系统必须认同在 IPSec 策略中使用的一个共享密钥,使用预先共享密钥仅当证书和 Kerberos 无法配置的场合。

3. 封装安全载荷协议 ESP

安全加载封装协议(ESP)通过对数据包的全部数据和加载内容进行加密来保证传输信息的机密性,这样可以避免其他用户通过监听打开信息交换的内容,因为只有受信任的用户拥有密钥打开内容。此外,ESP 也能提供身份认证、数据完整性验证和防止重发。在隧道模式中,整个 IP 数据报都在 ESP 负载中进行封装和加密。当该过程完成以后,真正的 IP 源地址和目的地址都可以被隐藏为 Internet 发送的普通数据。这种模式的一种典型用法就是在防火墙与防火墙之间通过 VPN 的连接进行的主机或拓扑隐藏。在传输模式中,只有更高层协议帧(TCP、UDP、ICMP 等)被放到加密后的 IP 数据报的 ESP 负载部分。在这种模式中,源地址和目的 IP 地址以及所有的 IP 包头域都是不加密发送的。

ESP 主要使用 DES 或 3DES 加密算法为数据包提供机密性。例如,使用计算机 A 的用户甲将数据发送给使用计算机 B 的用户乙。因为 ESP 提供机密性,所以数据被加密。接收端在验证过程完成后,数据包的数据部分将被解密。用户乙可以确定确实是用户甲发送的数据并且数据未经修改,其他人无法读取这些数据。

ESP 报头提供集成功能和 IP 数据的可靠性。集成功能保证了数据没有被恶意网客破坏,可靠性保证使用密码技术的安全。对 IPv4 和 IPv6,ESP 报头都列在其他 IP 报头后面。ESP 编码只有在不被任何 IP 报头扰乱的情况下才能正确发送包。

ESP 协议数据单元格式由 3 个部分组成,除了头部、加密数据部分外,在实施认证时还包含一个可选尾部。使用 ESP 进行安全通信之前,通信双方需要先协商好一组将要采用的加密策略,包括使用的算法、密钥以及密钥的有效期等。加密数据部分除了包含原 IP 数据包的有效负载,填充域(用来保证加密数据部分满足块加密的长度要求)包含其余部分在传输时都是加密过的。

5.4.3 IPSec 设置与应用实例

1. IPSec 的基本配置

AH 和 ESP 报头中没有指明用来产生认证数据和负载数据的算法,这意味着可以使用一些不同的算法。这样,如果出现了一个新的算法,系统可以不做明显改动地将该算法合成进 IPSec 标准中。目前,MD5 和 SHA 是用来产生认证数据的两种算法。ESP 使用的加密算法有 DES、3DES、RC5 和 IDEA。

一旦确定了 IPSec 安全级别,接下来就是配置 IPSec 安全性。IPSec 策略配置是把安全需求转换为一个或者多项 IPSec 策略,针对个人用户、工作组、应用系统、域、站点或跨国企业等不同的安全要求,网络安全管理员可以配置多种 IPSec 策略以分别满足其需求。每项 IPSec 策略包含一条或多条 IPSec 规则,每条 IPSec 规则包含一个过滤列表、过滤动作、认证方法以及连接类型等。

过滤列表决定了受安全规则制约的 IP 流量类型。一旦过滤器被触发,就会采取过滤动作。过滤动作指明了对应于过滤列表中所标出的 IP 地址所采取的安全措施。配置 IPSec 过滤动作时有以下 3 种可选动作。

(1) 允许

IPSec 安全策略中的允许选项是默认值。数据包允许在网络中传输,无需 IPSec 保护。

（2）阻塞

当使用阻塞过滤选项时，网络中不允许运行满足相应的 IP 过滤条件的协议。

（3）协商安全性

如果一项 IPSec 过滤条件得到匹配，协商安全性选项可以让管理员设置对数据的加密算法。

下面介绍 IPSec 的基本配置及选取不同算法的过程。

选择“开始”→“程序”→“管理工具”→“本地安全策略”菜单，打开“本地安全设置”对话框。单击“IP 安全策略：在本地机器”选项，如图 5.28 所示。最初窗口显示客户端、服务器、安全服务器这 3 种预定义的策略项。在每个预定义的策略的描述中详细解释了该策略的操作原则。如果想要修改系统预定义的策略细节，可以右击相应的策略并选择“属性”进行修改。



图 5.28　打开本地安全设置

（1）创建 IP 安全策略

第 1 步：右击“IP 安全策略，在本地机器”选项，选择“创建 IP 安全策略”项，如图 5.29 所示；打开如图 5.30 所示的“安全策略向导”对话框，单击“下一步”按钮继续。

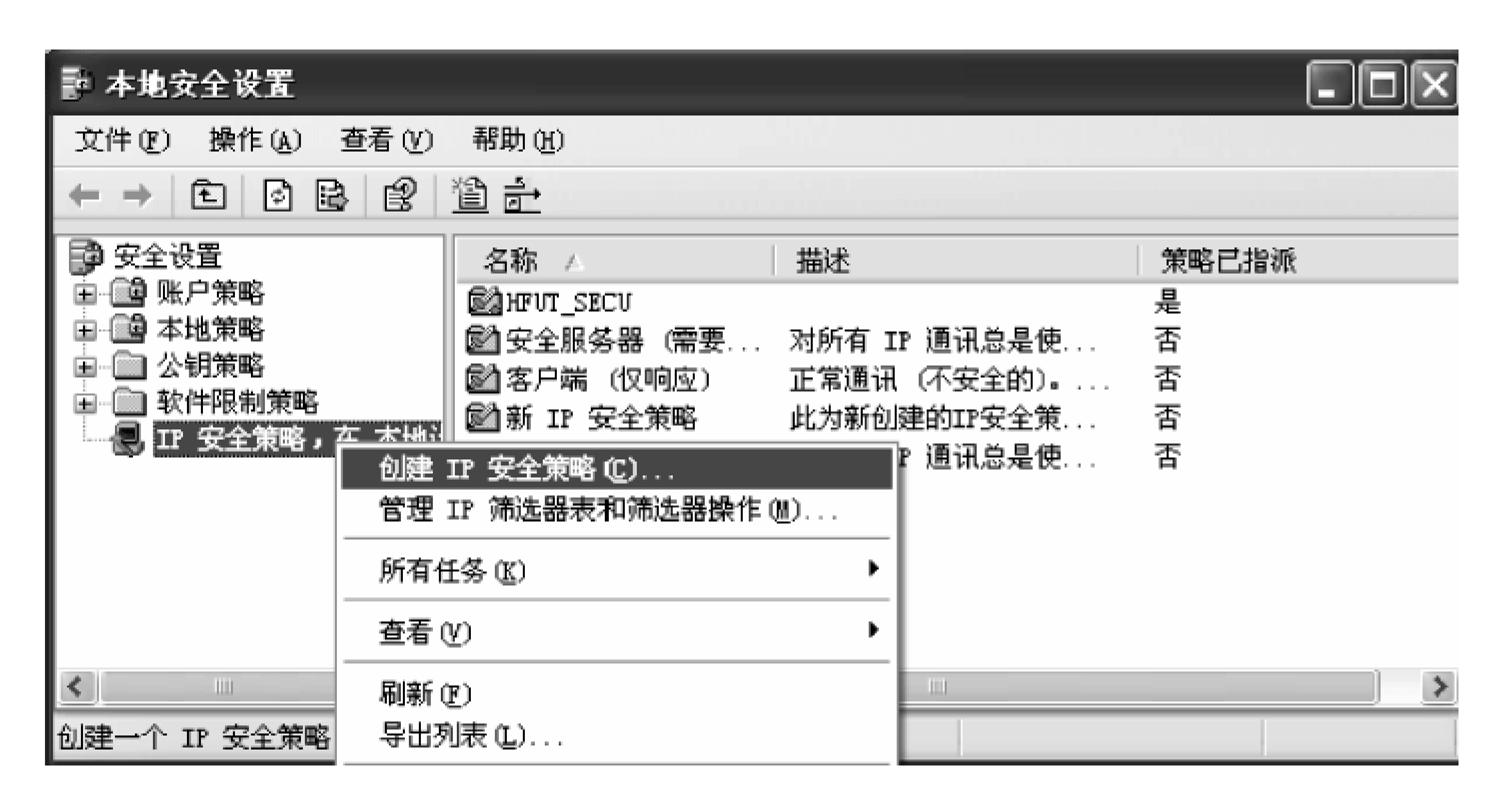


图 5.29　创建 IP 安全策略

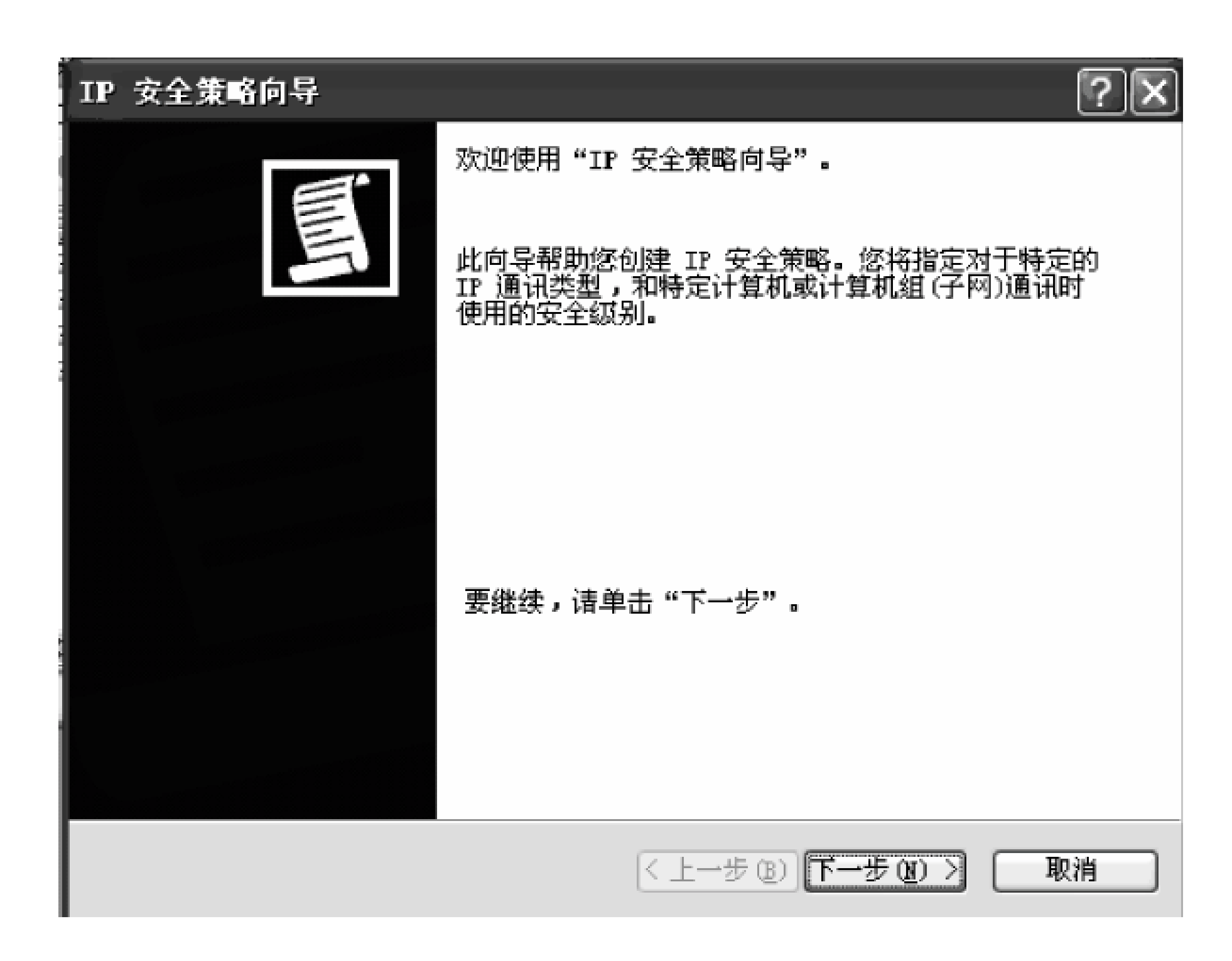


图 5.30　安全策略向导

第 2 步：在弹出的对话框中为新的 IP 安全策略命名并填写策略描述，如图 5.31 所示。

IP 安全策略向导
IP 安全策略名称
命名这个 IP 安全策略并且给出一个简短的描述
名称(M)：
新 IP 安全策略
描述(D)：
此为新创建的IP安全策略，该策略可以......
< 上一步(B)　下一步(N) >　取消

图 5.31　“IP 安全策略名称”对话框

第 3 步：单击“下一步”按钮，选择“激活默认响应规则”复选项，如图 5.32 所示，然后单击“下一步”按钮。

第 4 步：接受默认的选项“Active Directory 默认值(Kerberos V5 协议)”作为默认响应规则身份验证方法，如图 5.33 所示，单击“下一步”按钮继续。

第 5 步：选中“编辑属性”复选框，并单击“完成”按钮，如图 5.34 所示。这样就完成了 IPSec 的初步配置。

完成初步配置后，将弹出新 IP 安全策略向导对话框，如图 5.35 所示。



图 5.32　“安全通信请求”对话框

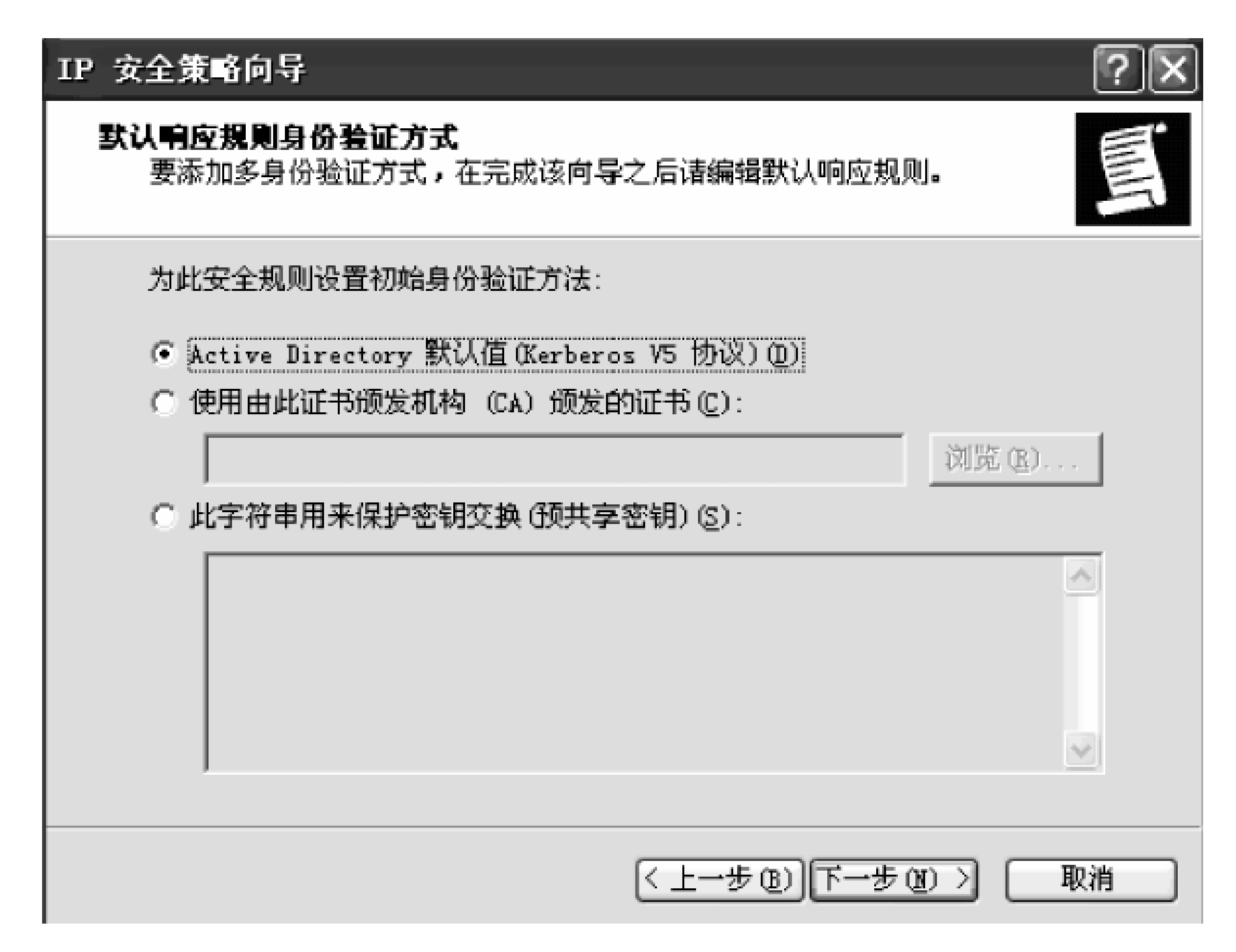


图 5.33　设置身份验证方法

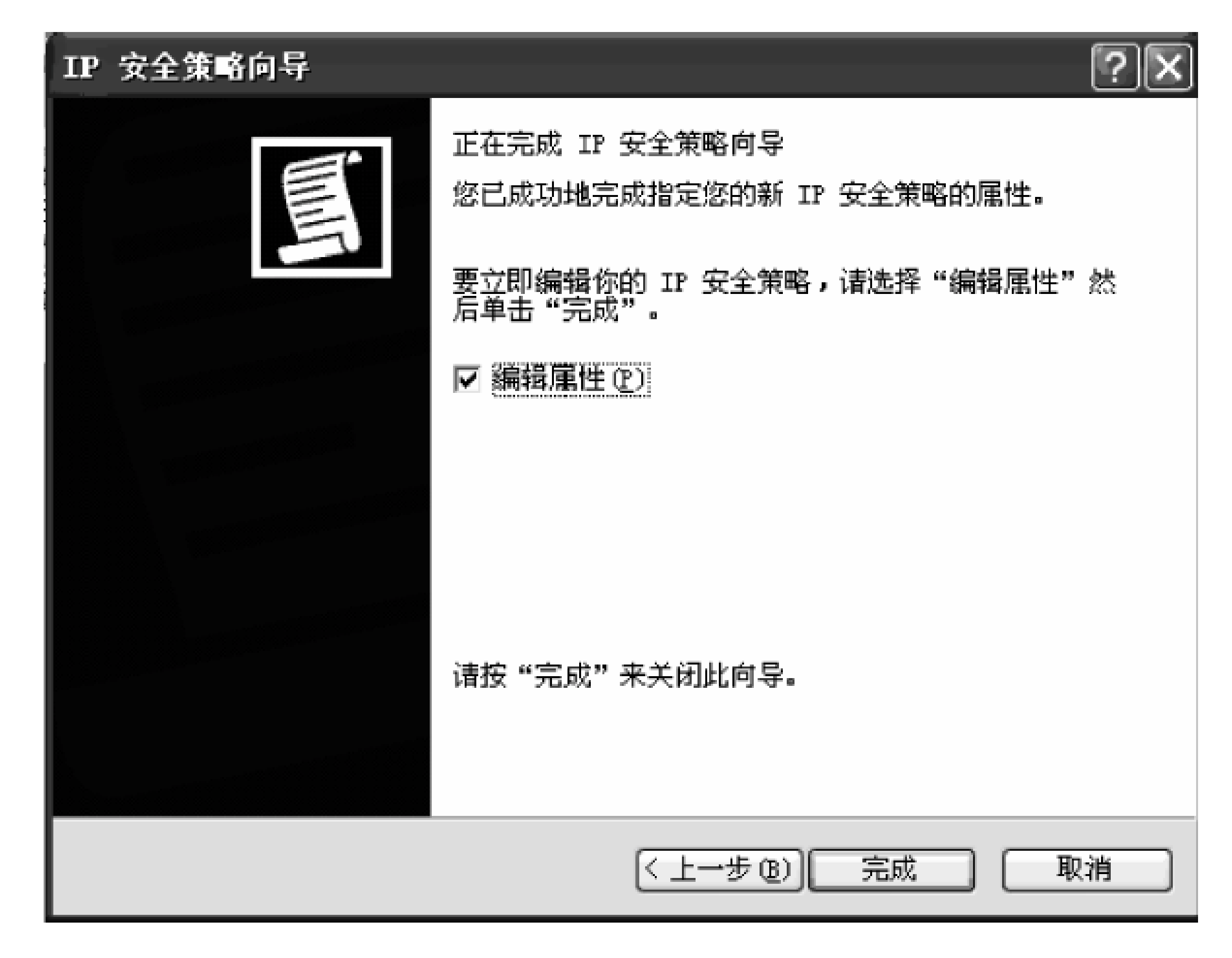


图 5.34　完成 IP 安全策略向导

(2) 配置安全策略和规则

用户添加自己定义的“IP 安全规则”。在不选择“使用‘添加向导’”情况下(撤销图 5.35 下面复选框中的“√”),单击“添加”按钮,弹出如图 5.36 所示的“新规则 属性”对话框。在这里用户就可以对新规则的各项属性进行如下设置。



图 5.35 “新 IP 安全策略 属性”对话框

图 5.36 “新规则 属性”对话框

① IP 筛选列表设置

第 1 步:在如图 5.37 所示的“IP 筛选列表”对话框上单击“添加”按钮,打开“IP 筛选器列表”对话框。

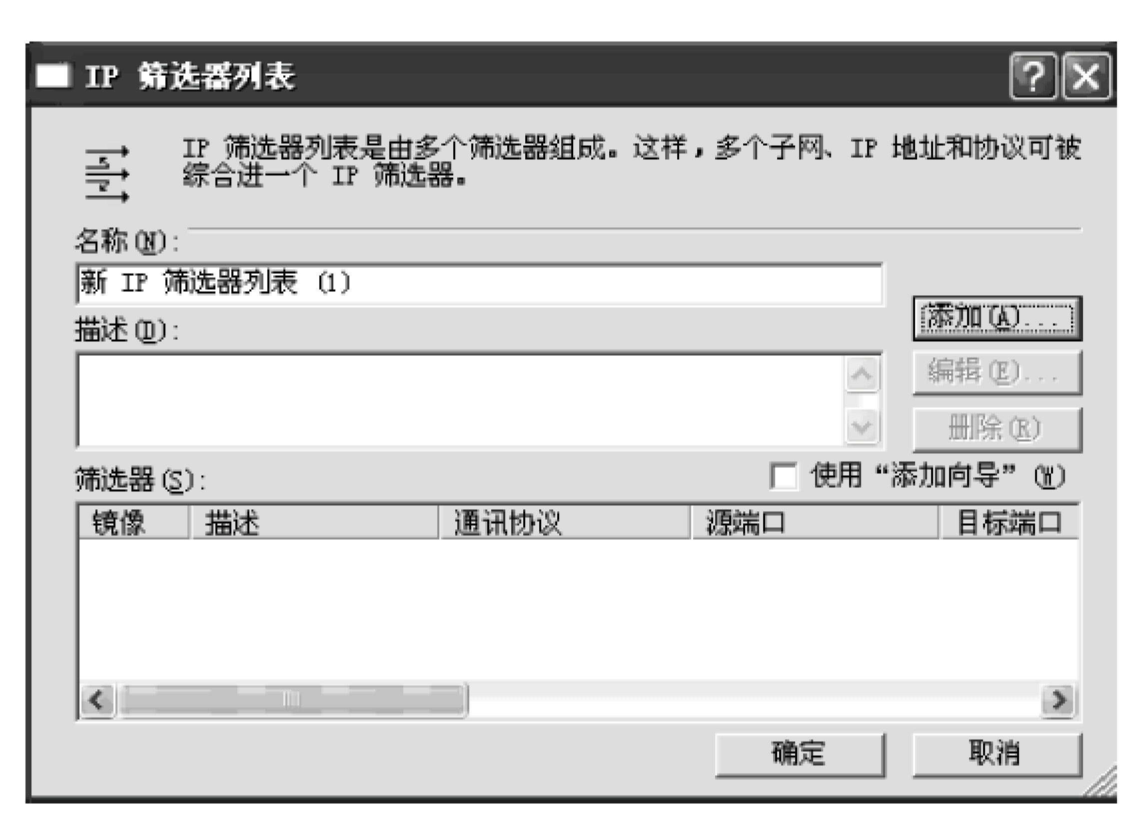


图 5.37 “IP 筛选器列表”对话框

第 2 步:输入新 IP 筛选器列表的名称、描述信息并在不选择“使用‘添加向导’”情况下,单击“添加”按钮,弹出如图 5.38 所示的“筛选器 属性”对话框。筛选器属性包含寻址、协议和描述 3 个选项卡:“寻址”选项卡可对 IP 数据流的源地址、目标地址进行规定;“协议”选项卡可对数据流所使用的协议进行规定,如果选择了 TCP 或 UDP 协议,还可以对源端和目的端使用的端口号做出规定;“描述”选项卡可对新筛选器做出简单描述。

第 3 步：在图 5.38 的“寻址”选项卡中选择 IP 数据流的源地址和目标地址。

第 4 步：打开“协议”选项卡后，在图 5.39 窗口中可选择协议类型，如选择 ICMP 或 TCP 等。

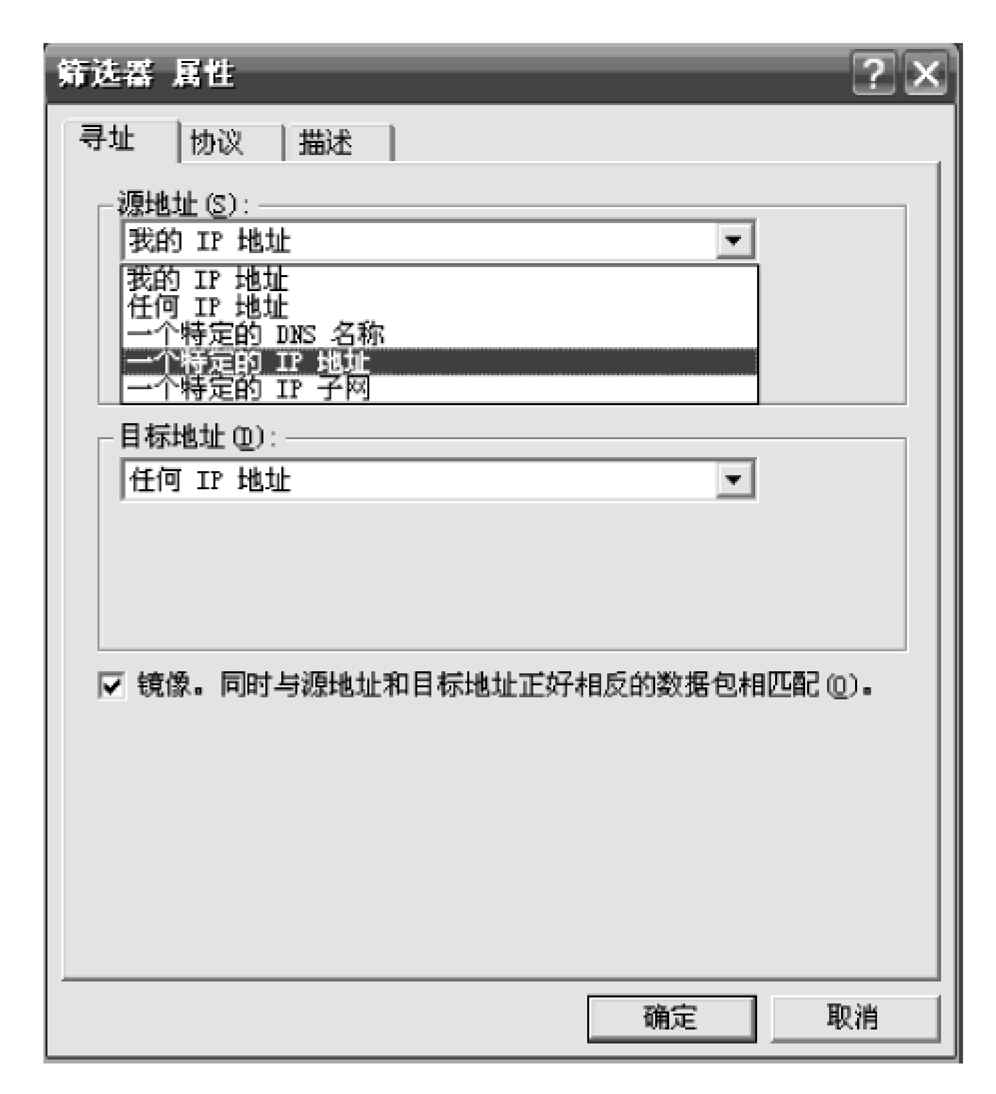


图 5.38　“筛选器 属性”对话框





图 5.39　筛选器 属性——协议

第 5 步：单击“确定”按钮后，完成对“筛选器 属性”的设置，然后要确保选中新设置的 IP 筛选器，如图 5.40 所示。

② 筛选器操作设置

“筛选器操作”选项卡是整个 IPSec 设计的关键，它将对符合“IP 筛选器”的数据流进行相应的处理。

第 1 步：选择图 5.40 中的“筛选器操作”选项卡，如图 5.41 所示。在此不选择“使用‘添加向导’”情况下单击“添加”按钮，弹出如图 5.42 所示的“新规则 属性”对话框。

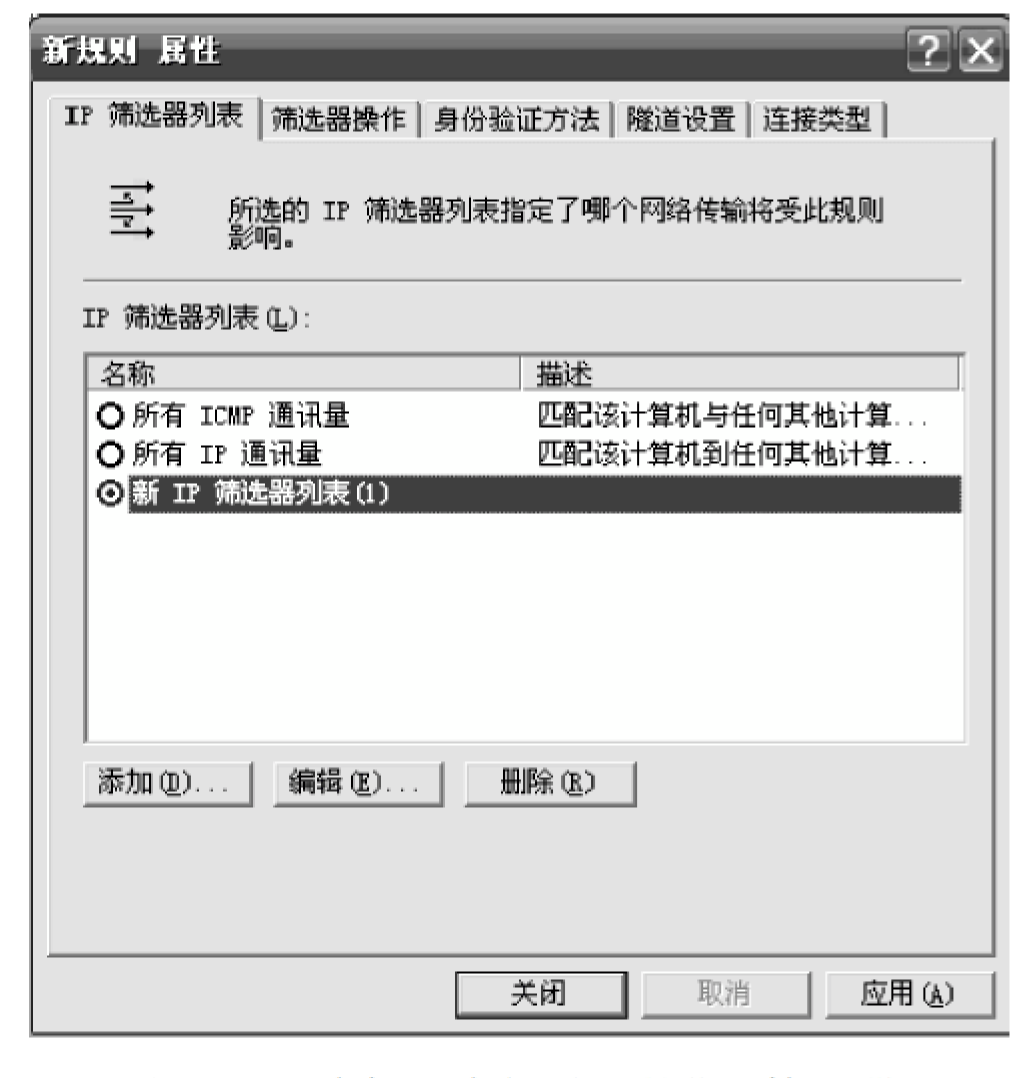


图 5.40　确保选中新设置的“IP 筛选器”



图 5.41　“新筛选器操作 属性”对话框

第 2 步：在这里可以对新筛选器操作的细节进行设置。其中，可以选择“许可”、“阻止”对符合“IP 筛选器”的数据流进行过滤。此处选择“协商安全”选项，以便对允许的通信进行进一步的安全设置。

第 3 步：单击“添加”按钮，弹出如图 5.43 所示的“安全措施”窗口，选择添加相应的安全措施。可选的安全措施有“加密并保持完整性”、“仅保持完整性”和“自定义”3 种。



图 5.42 “筛选器操作”选项卡

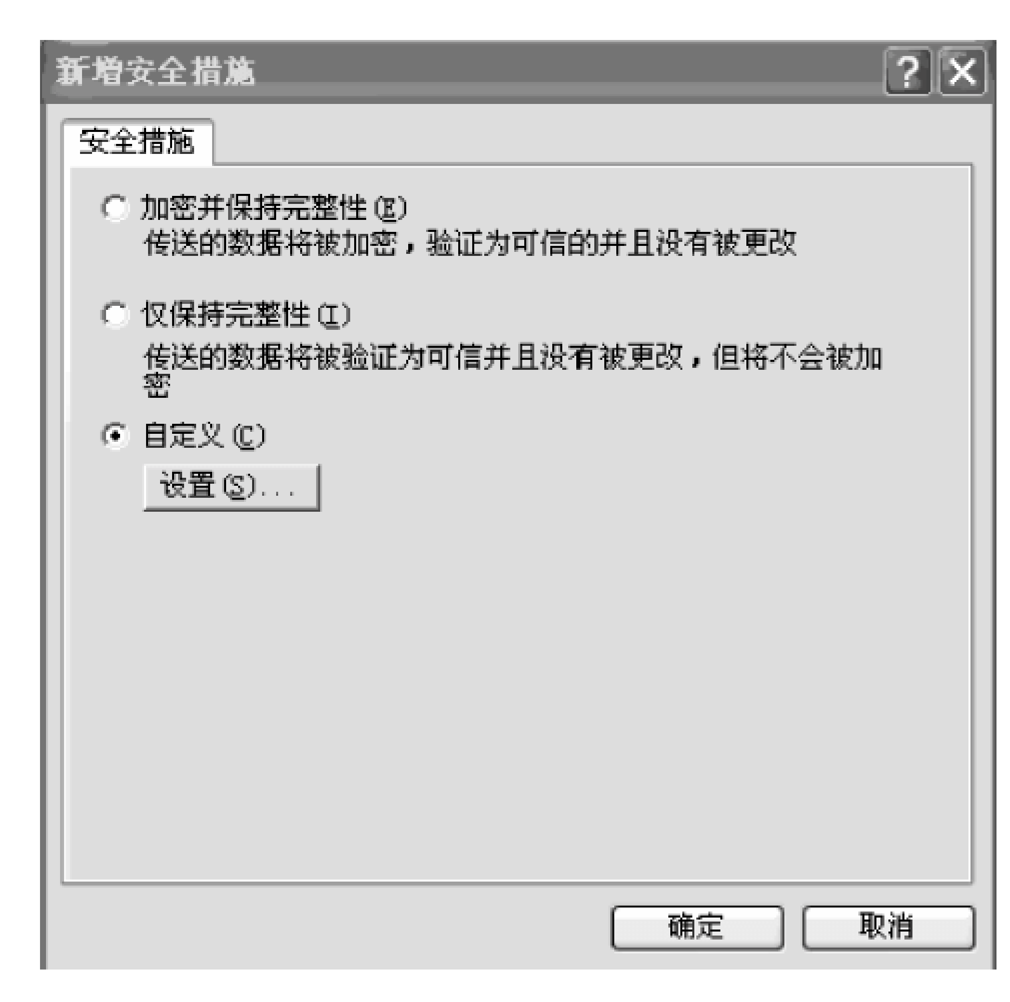


图 5.43 “安全措施”选项卡

第 4 步：自定义包括数据和地址不加密的完整性算法、数据完整性算法(如 MD5、SHA1)、数据加密算法(如 DES、3DES)和密钥生存期等。在此选择“自定义”选项，再单击“设置”按钮，出现如图 5.44 所示的窗口，用户可按要求进行选择。

第 5 步：单击“确定”按钮后，弹出如图 5.45 所示的窗口，在此可以添加多个安全措施，并通过“上移”、“下移”按钮指定和另一计算机协商时采取的安全措施首选的顺序，并可对某次设置进行修改和删除。



图 5.44 “自定义安全措施设置”对话框

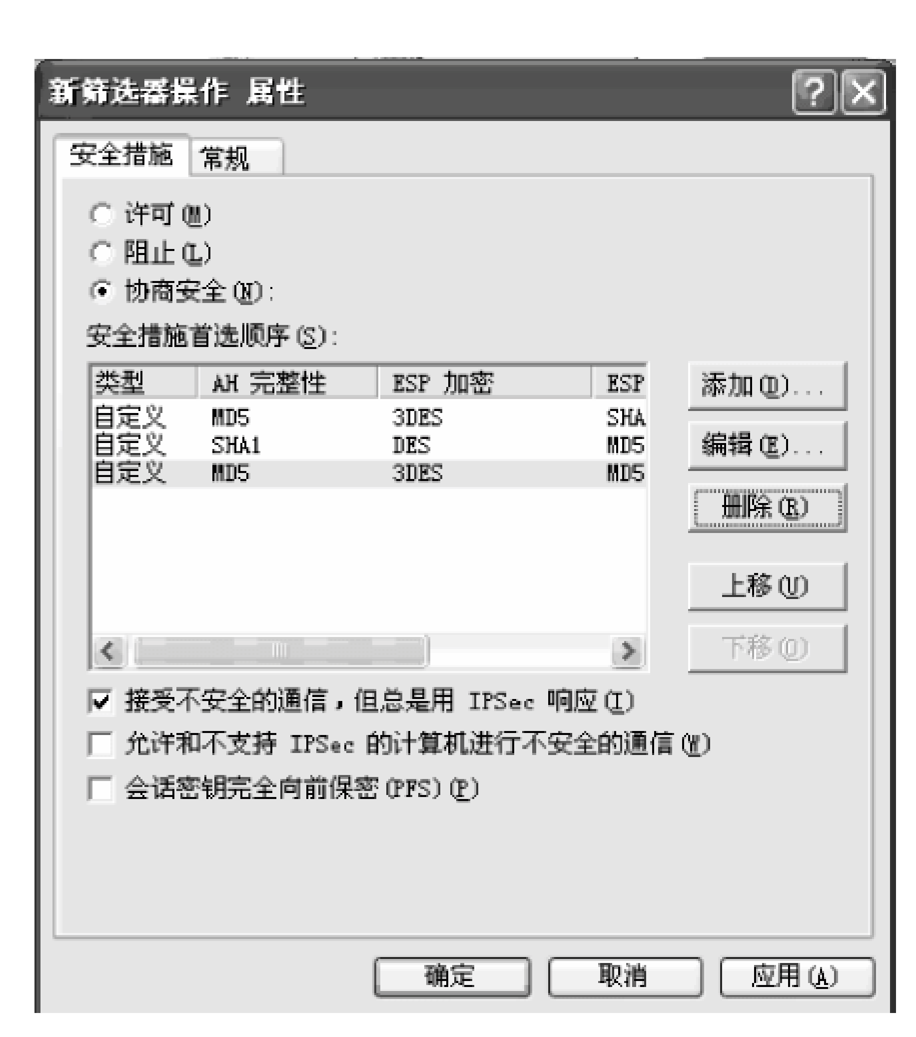


图 5.45 添加多个安全措施

在图 5.45 所示“安全措施”选项卡中还有如下三个选项。

- 接受不安全的通信，但总是用 IPSec 响应：接受由其他计算机初始化的不受保护的通信，但在本机应答或初始化时总是使用安全的通信。
- 允许和不支持 IPSec 的计算机进行不安全的通信：允许来自或到其他计算机的不受保护的通信。
- 会话密钥完全向前保密：确保会话密钥和密钥材料不被重复使用。

注意：当以上内容设置结束，单击“确定”按钮回到“筛选器操作”选项卡后，必须选中刚才添加的新筛选器操作项，如图 5.46 所示。

③ 身份验证方法设置

身份验证方法定义了向每一位用户保证其他的计算机或用户的身份。每一种身份验证方法都提供必要的手段来保证身份。

第 1 步：单击图 5.46 中的“身份验证方法”选项卡，弹出如图 5.47 所示的窗口。



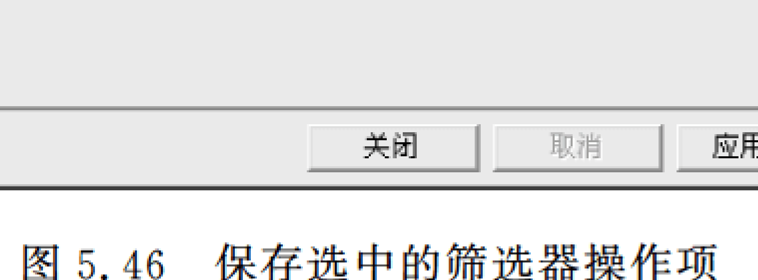


图 5.46 保存选中的筛选器操作项



图 5.47 “身份验证方法”选项卡

第 2 步：选择身份验证方法。Windows 2000/XP/2003 支持 3 种身份验证方法：Kerberos v5 协议、CA 证书和预共享密钥，如图 5.48 所示。

④ 隧道设置

单击“隧道”选项卡，弹出如图 5.49 所示的窗口。当只与特定的计算机交换通信并且知道该计算机的 IP 地址时，选择“隧道终点由此 IP 地址指定”并输入目标计算机的 IP 地址。

⑤ 连接类型

为每一个规则指定的连接类型可以决定计算机的连接（网卡或调制解调器）是否接受 IPSec 策略的影响。每一个规则拥有一种连接类型，此类型指定规则是否应用到 LAN 连接、远程访问连接或所有的网络连接上，如图 5.50 所示。

（3）新 IP 属性的常规设置

第 1 步：新创建的 IP 安全策略属性对话框还有一个“常规”选项卡。在此可以输入新 IP 安全策略的名称和描述，更改“检查策略更改间隔”，如图 5.51 所示。

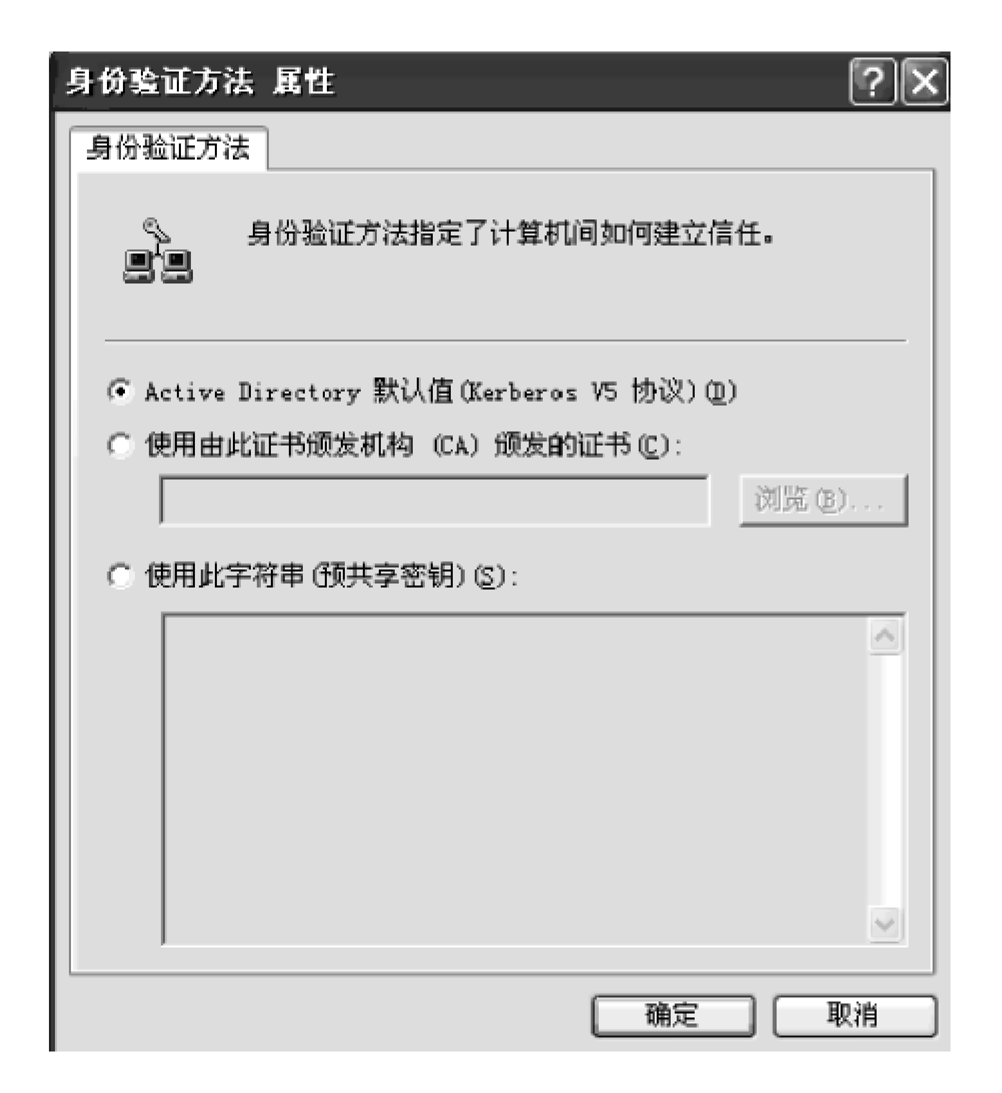


图 5.48 “身份验证方法 属性”对话框

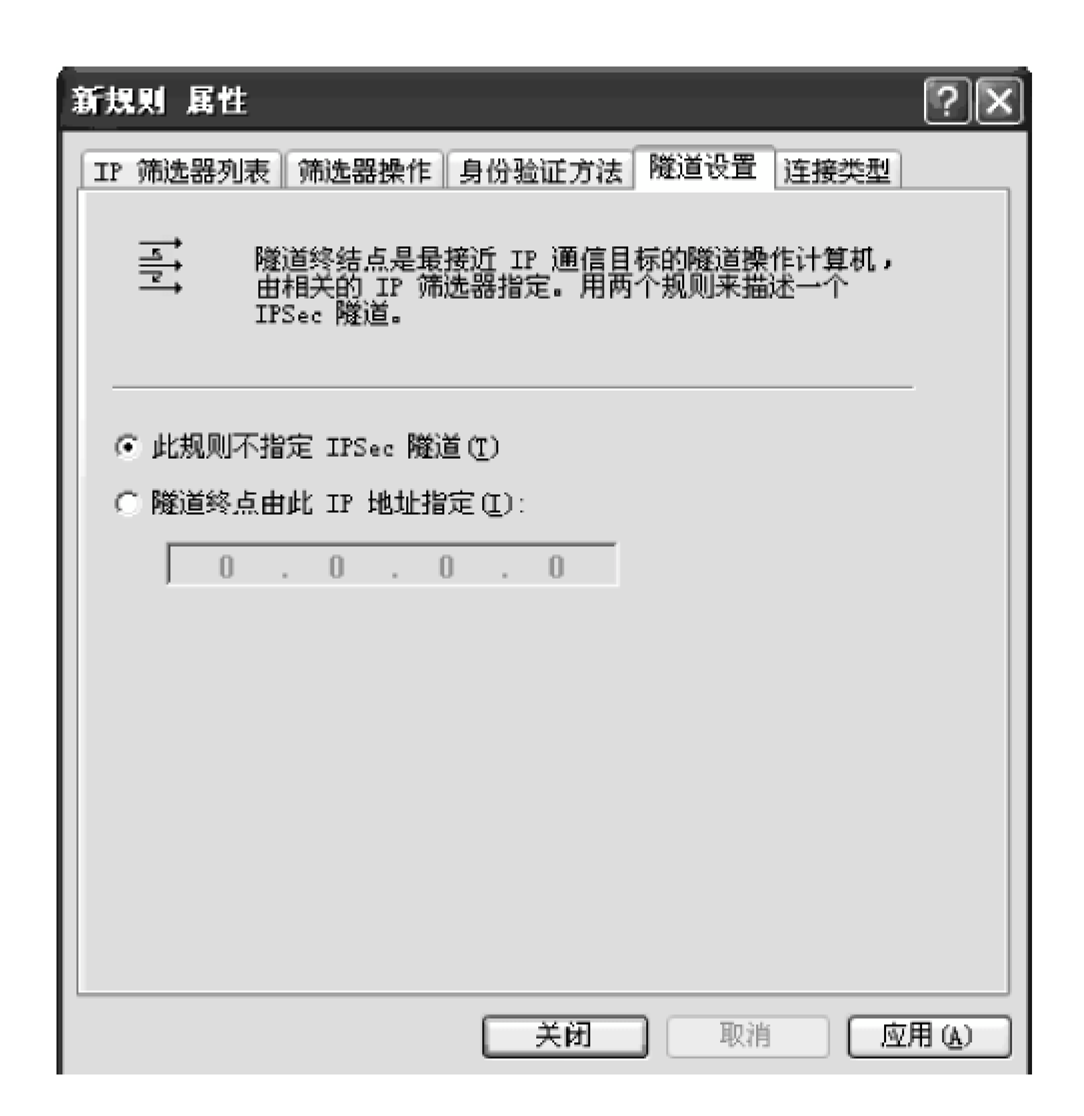


图 5.49 “隧道设置”选项卡



图 5.50 “连接类型”选项卡



图 5.51 “新 IP 安全策略 属性”对话框的“常规”选项卡

第 2 步：单击“高级”按钮，在弹出的如图 5.52 所示的“密钥交换设置”对话框中对密钥交换进行高级设置。其中：

- 主密钥完全向前保密：选择保证没有重用以前使用的密钥材料或密钥来生成其他主密钥。
- 身份验证和生成新密钥间隔(A)：确定在其后将生成新密钥的时间间隔。
- 身份验证和生成新密钥间隔(U)：限制主

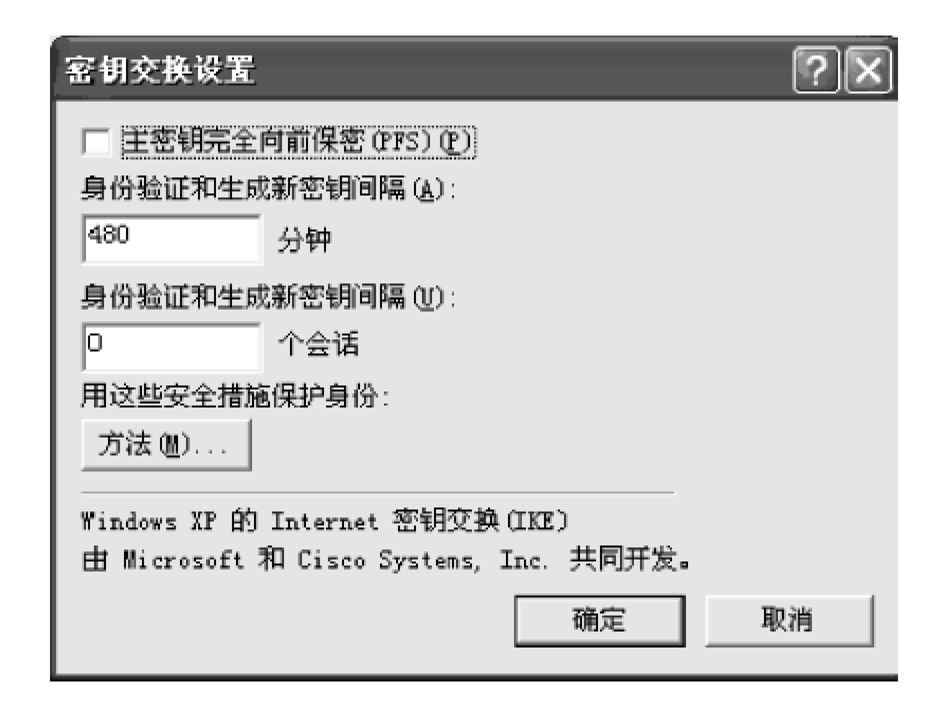


图 5.52 “密钥交换设置”对话框

密钥可以被作为会话密钥来重新使用的次数。如果已经启用了“主密钥完全向前保密”，则会忽略该参数。

- 用这些安全措施保护身份：单击“方法”按钮，在弹出的“密钥交换安全措施”对话框中对安全措施首选顺序以及 IKE 安全算法细节做出选择。其中完整性算法可选 MD5 或 SHA-1，加密算法可选 3DES 或 DES。

2. IPSec 的防火墙配置

Windows 系统可提供给用户免费使用的防火墙，它不同于通常所说的内置防火墙，但是却可以提供更好的安全策略，这就是 IP Filter。IP Filter 包含于 IPSec 中，是 Windows 2000 以后新加入的技术。其原理很简单，当接收到一个 IP 数据包时，IP Filter 使用其头部在一个规则表中进行匹配。当找到一个相匹配的规则时，IP Filter 就按照该规则制定的方法对接收到的 IP 数据包进行处理。这里的处理工作只有丢弃或转发两种选择。

IP Filter 只是 IPSec 的一部分功能。对于不在域中的个人用户，IPSec 的数据加密是用不到的。下面介绍如何用 IP Filter 构建防火墙，实现常用防火墙的部分功能。

(1) IP Filter 防火墙配置的准备工作

由于 IP Filter 属于 IPSec 的一部分，所以在使用及配置 IP Filter 前需要保证 IPSec 服务的正常运行。

第 1 步：单击“开始”→“运行”命令，输入 services.msc 并按回车键，进入服务设置窗口。在服务设置窗口中找到名为 IPSEC Services 的服务，保证它是启动的，如图 5.53 所示。



图 5.53　服务设置窗口

第 2 步：如果该服务没有启动，则双击其名称，可单击“启动”按钮启动该服务，然后再将其启动方式设置为“自动”，这样才能保证下面设置好的 IP Filter 防火墙过滤信息可以随系统启动而启动，从而保证对数据包的过滤功能生效，如图 5.54 所示。

如果用户在服务名称中没有找到 IPSEC Services 服务也不要紧，该项服务可以在 Windows 2000 全系列/XPPro/.NetServer 中找到。



图 5.54 IPSEC Services 属性

(2) 配置 IP Filter

有过配置防火墙或过滤策略经历的读者在配置 IP Filter 上也是非常容易的。配置策略和访问控制列表以及过滤规则是一样的。可通过 MMC 加载 IPSec 模块来实施此功能。

第 1 步：单击“开始”→“运行”命令，输入 MMC 并按回车键，启动管理单元控制台窗口，如图 5.55 所示。



图 5.55 控制台窗口

第 2 步：默认情况下只有“控制台根节点”一个选项。可通过主菜单的“文件”下拉后选择“添加/删除管理单元”选项来加载 IPSec 模块。

第 3 步：在出现的“添加/删除管理单元”对话框的“独立”选项卡下单击“添加”按钮，如图 5.56 所示。

第 4 步：在弹出的如图 5.57 所示的“添加独立管理单元”选项中选择“IP 安全策略管

理”，单击“添加”按钮进行添加。



图 5.56　“添加/删除管理单元”对话框



图 5.57　“添加独立管理单元”对话框

第 5 步：系统会要求用户选择的这个管理单元要管理的计算机或者域。由于这里是对本地计算机操作的，所以选择“本地计算机”后单击“完成”按钮，如图 5.58 所示。

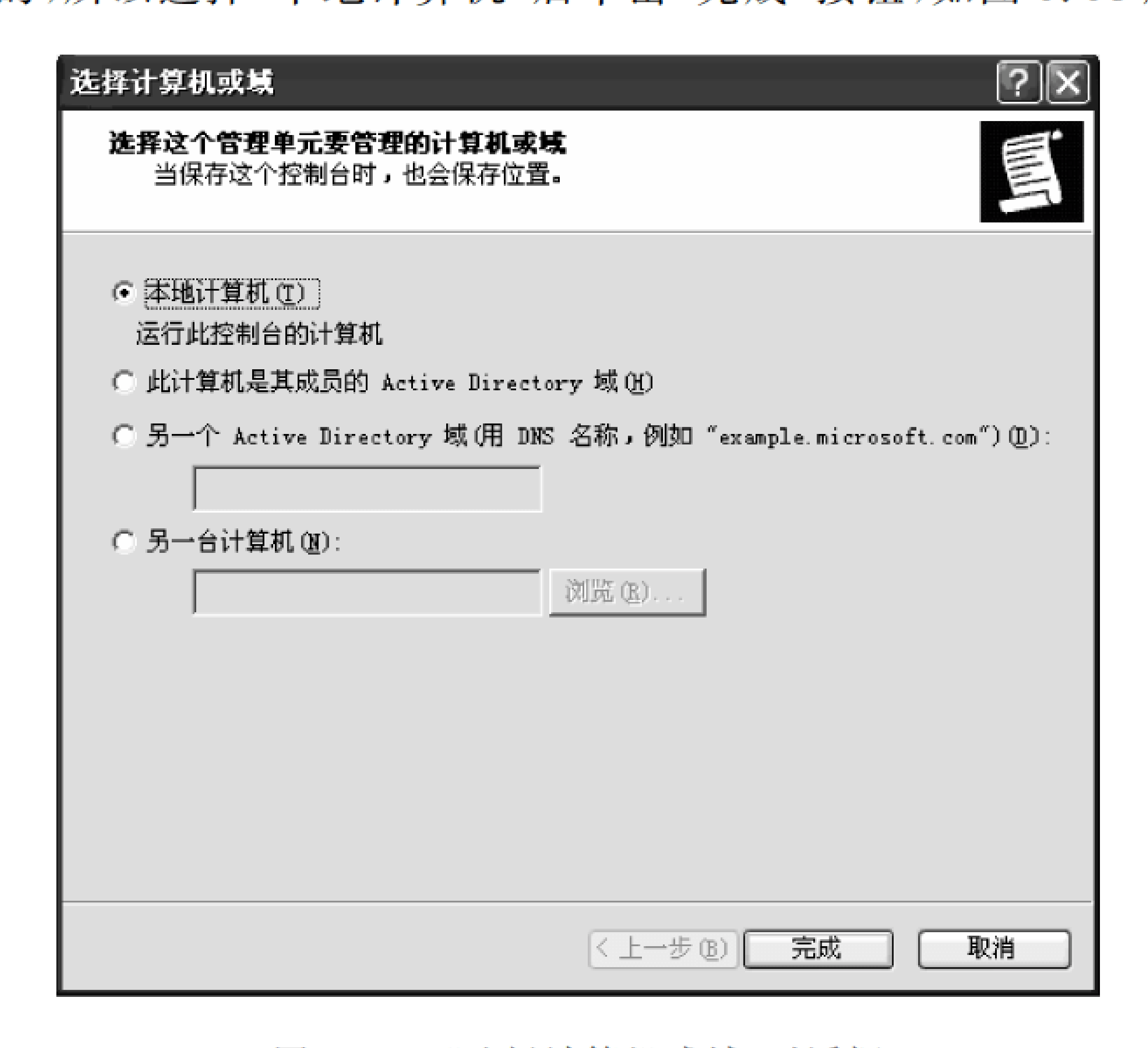


图 5.58　“选择计算机或域”对话框

第 6 步：添加后就可在控制台窗口的“控制台根节点”下看到“IP 安全策略，在本地计算机”项，如图 5.59 所示。在“IP 安全策略，在本地计算机”上右击并选择“管理 IP 筛选器表和筛选器操作”开始配置防火墙策略，如图 5.60 所示。

用户也可以单击“开始”→“运行”命令后，输入 secpol.msc 并按回车键，在打开的窗口中

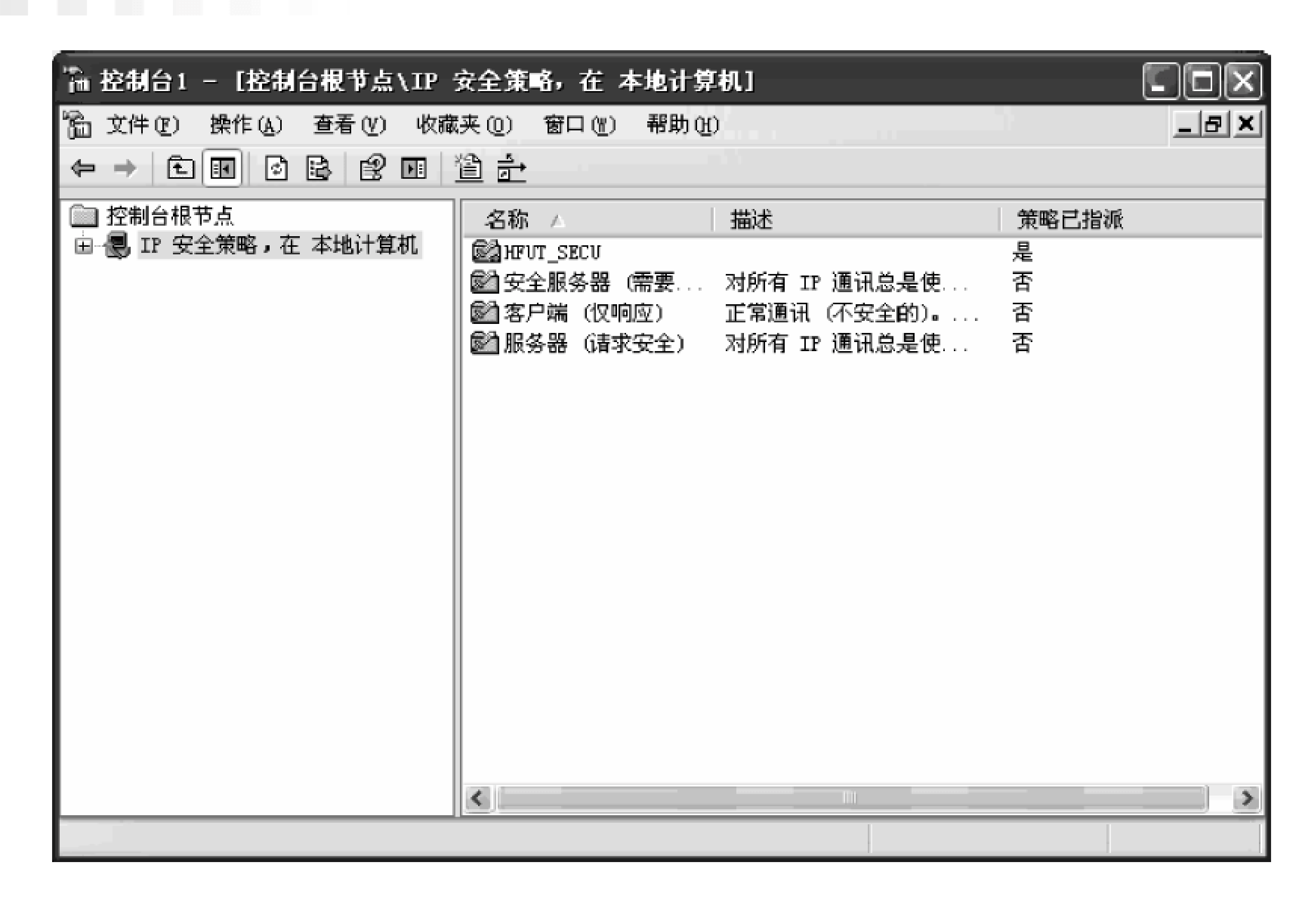


图 5.59 添加 IP 安全策略

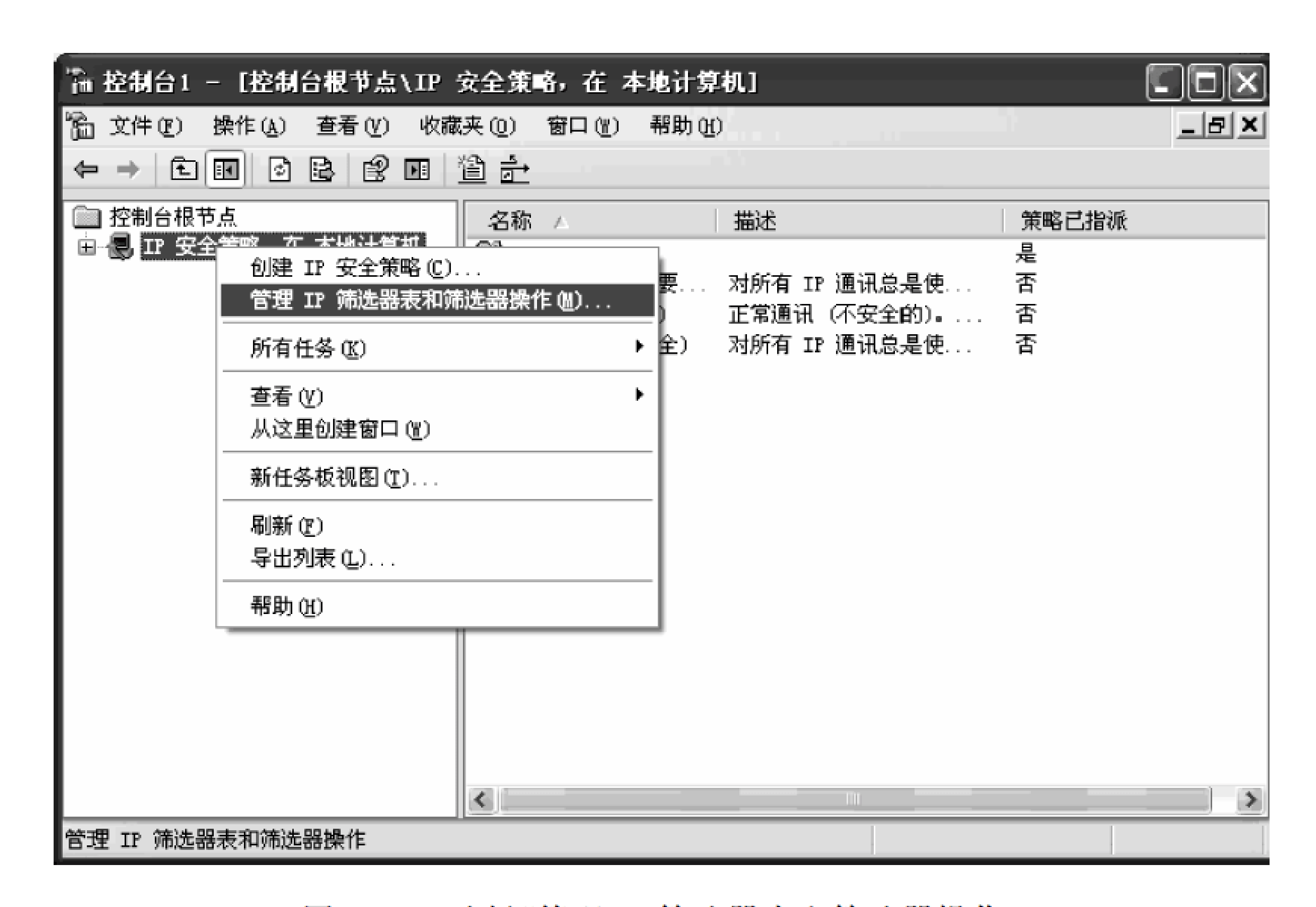


图 5.60 选择"管理 IP 筛选器表和筛选器操作"

可以直接选择"管理 IP 筛选器表和筛选器操作"。这种方法更加简单快捷。

第 7 步：在弹出的"管理 IP 筛选器表和筛选器操作"设置窗口中，默认情况下有对"所有 ICMP 通信量"和对"所有 IP 通信量"进行过滤的。可以通过"添加"按钮添加新的规则，如图 5.61 所示。

第 8 步：系统会自动生成一个名为"新 IP 筛选器列表"的规则，可在该窗口中单击"添加"按钮，继续加入一个具体的过滤项，如图 5.62 所示。

第 9 步：系统将自动启动 IP 筛选器向导，单击"下一步"按钮，弹出如图 5.63 所示选择 IP 地址的窗口。

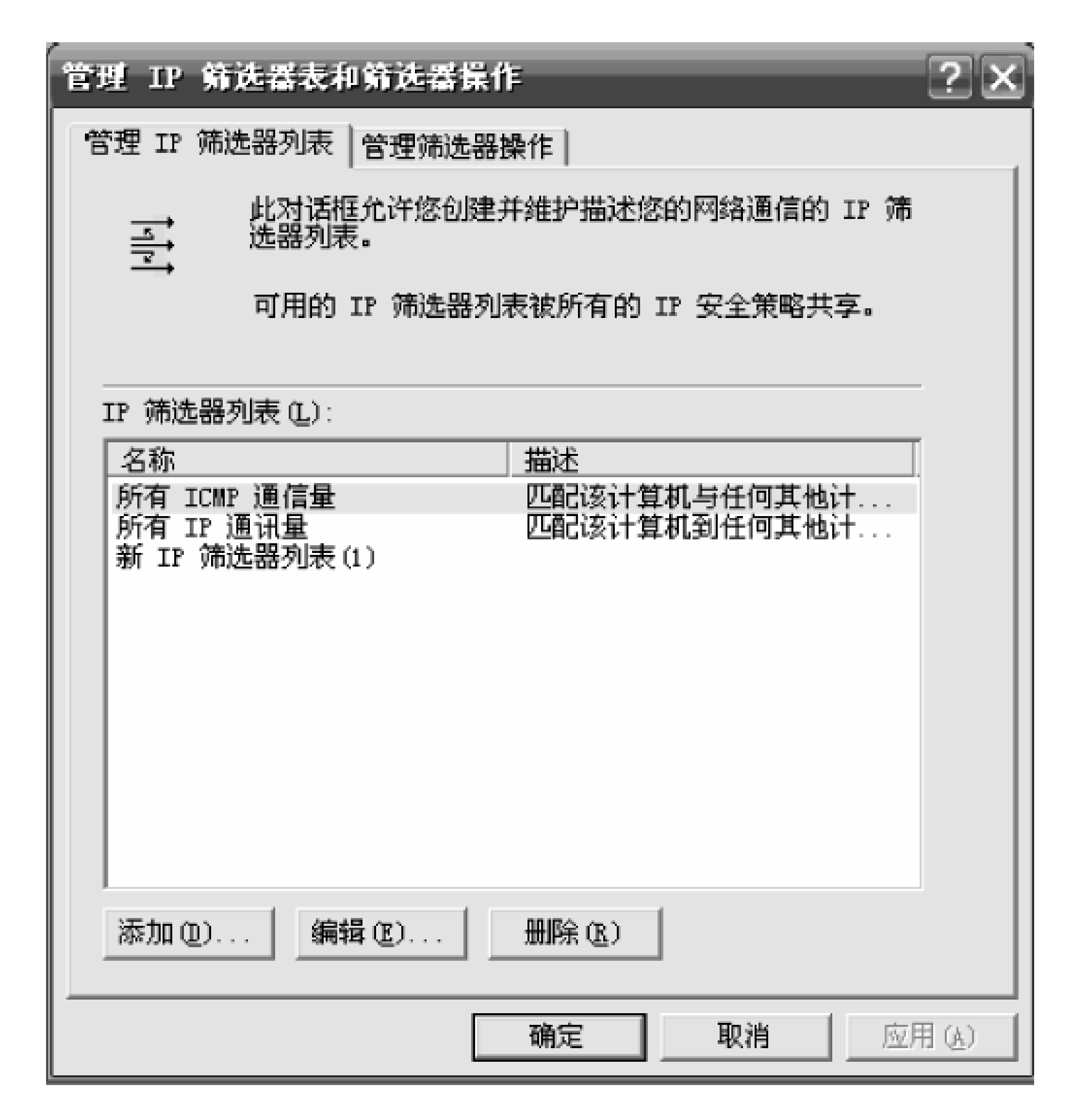


图 5.61　“管理 IP 筛选器表和筛选器操作”对话框

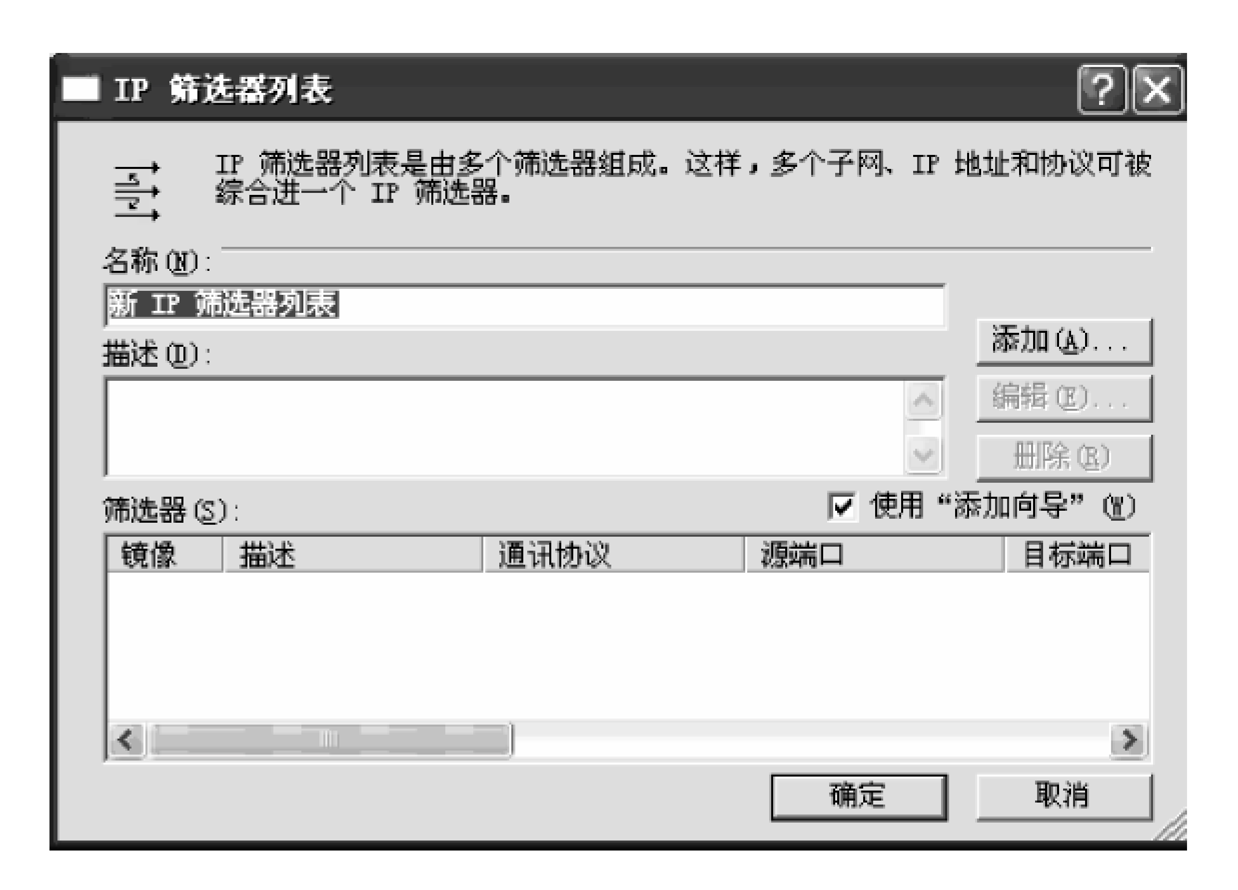


图 5.62　添加“IP 筛选器列表”

图 5.63　选择 IP 源地址窗口

第 10 步：指定 IP 通信的源地址，类似于规则中的源地址。可供选择的有特定的 IP 子网、特定的 IP 地址、特定的 DNS 名称、任何 IP 地址和本机 IP 地址。如果选择子网，会出现需要填写 IP 地址和子网掩码的对话框；如果选择 IP 地址，则出现要填写的 IP 地址框；如果选择 DNS 名称，则出现需填写主机名的框。

第 11 步：设置完后单击“下一步”按钮继续，弹出如图 5.64 所示的指定 IP 通信的目的地址窗口。可供选择的目的地址类似源地址，有特定的 IP 子网、特定的 IP 地址、特定的 DNS 名称、任何 IP 地址和本机 IP 地址。当用户想对某个域名进行过滤时，可以在目的地址处选择“一个特定的 DNS 名称”，然后在主机名处输入对应的域名，如 www.163.com（见图 5.64）。设置完后单击“下一步”按钮继续。

图 5.64　选择 IP 目标地址窗口

第 12 步：由于与 www.163.com 对应的有很多 IP 地址，而且是动态的，因此系统会首先查看本地 DNS 缓存，读取缓存中对应的 IP 地址进行过滤，如图 5.65 所示。

第 13 步：选择通信协议类型，包括常用的 TCP 和 UDP，还可以设置为任意，如图 5.66 所示。

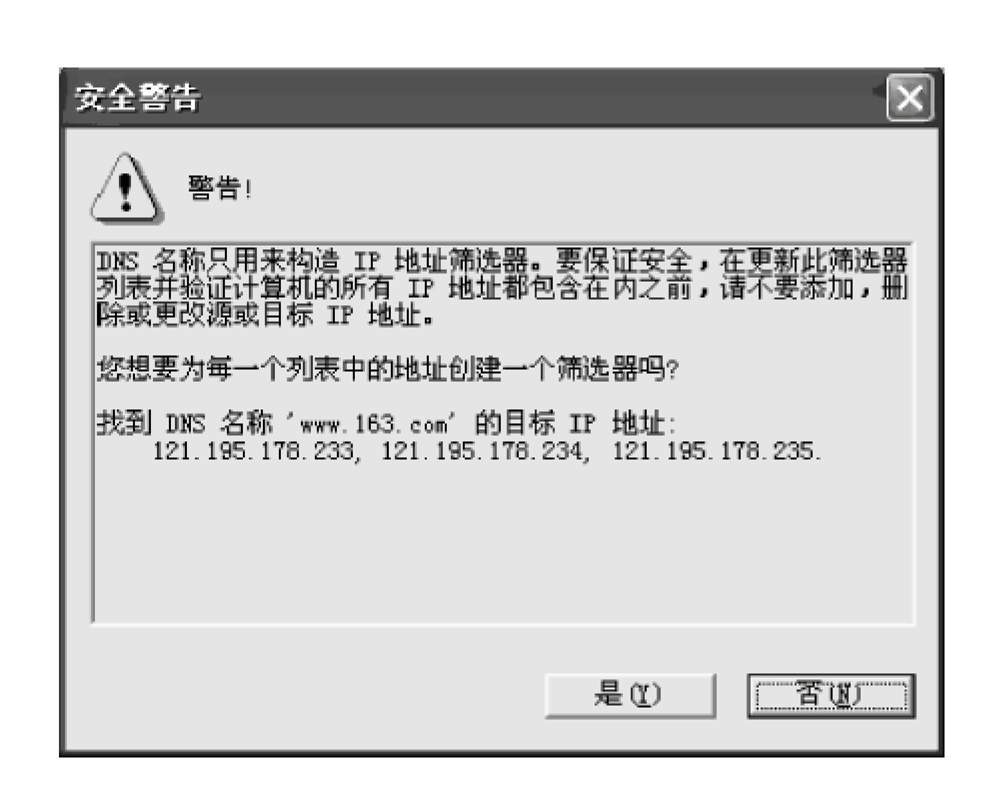


图 5.65　一个域名多 IP 地址警告

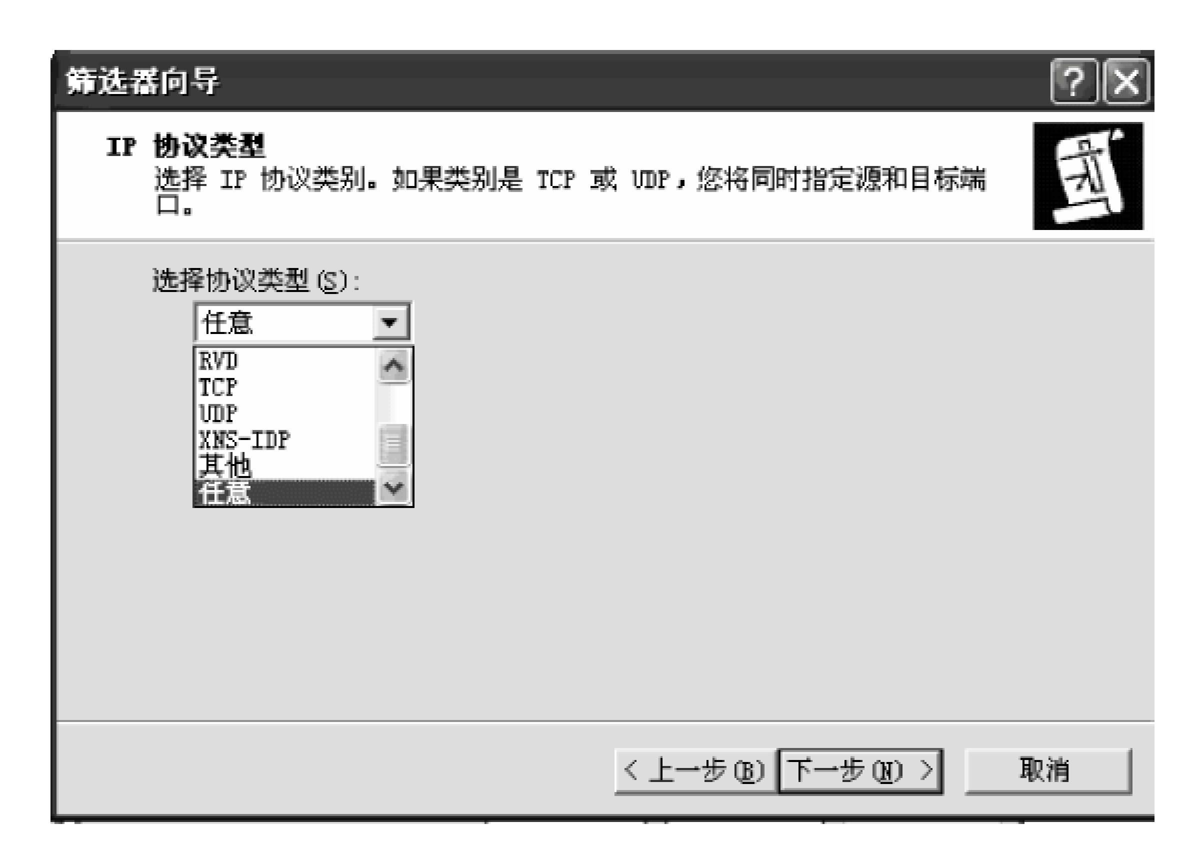


图 5.66　选择通信协议类型

第 14 步：单击“下一步”按钮后弹出完成 IP 筛选器建立向导窗口，单击“完成”按钮结束操作，如图 5.67 所示。

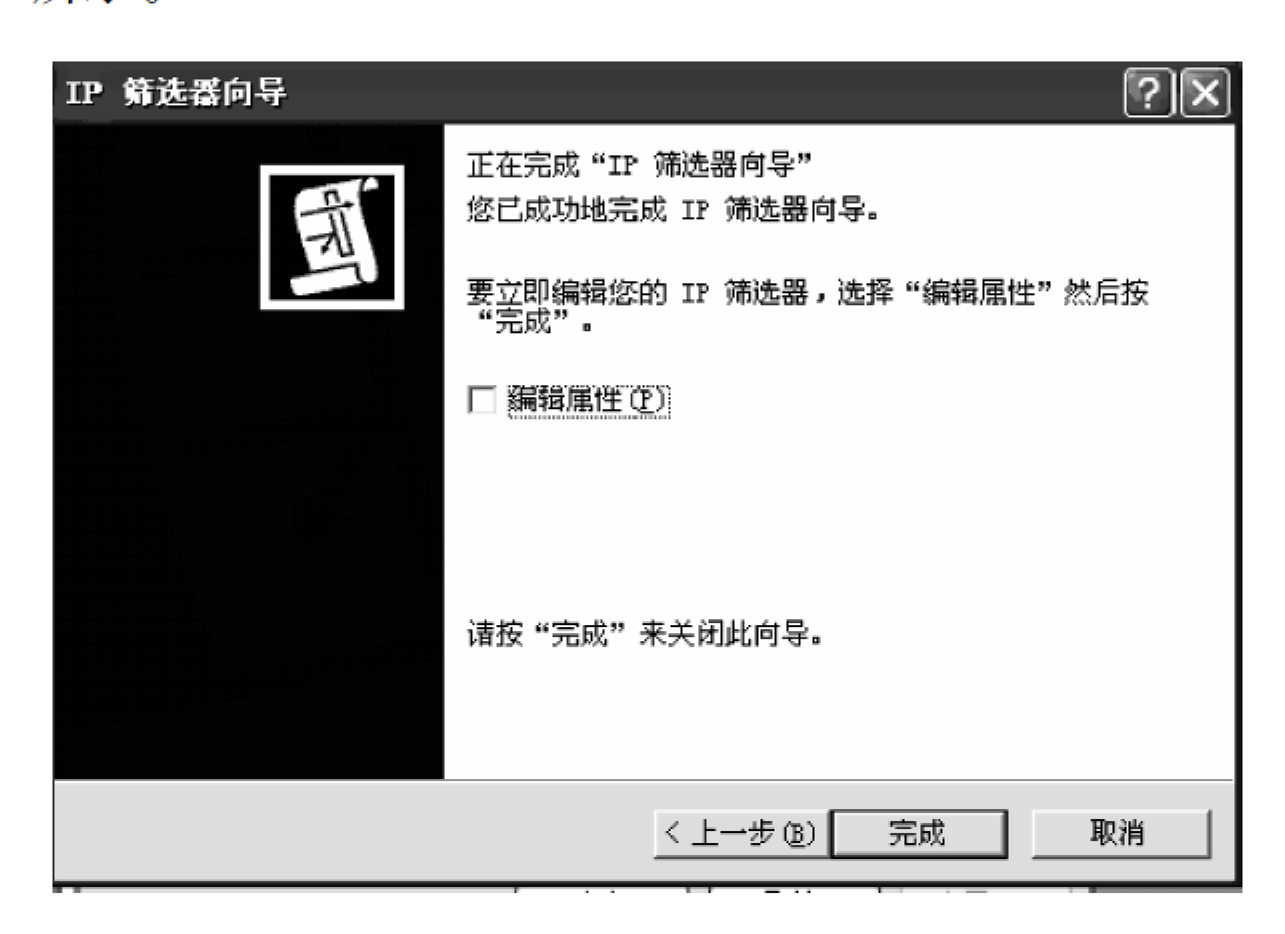


图 5.67　完成 IP 筛选器建立向导

第 15 步：这时可在刚刚见过的 IP 筛选器列表窗口中看到添加的规则。由于这些规则都是在同一个筛选器中，所以规则可以同时生效，如图 5.68 所示。

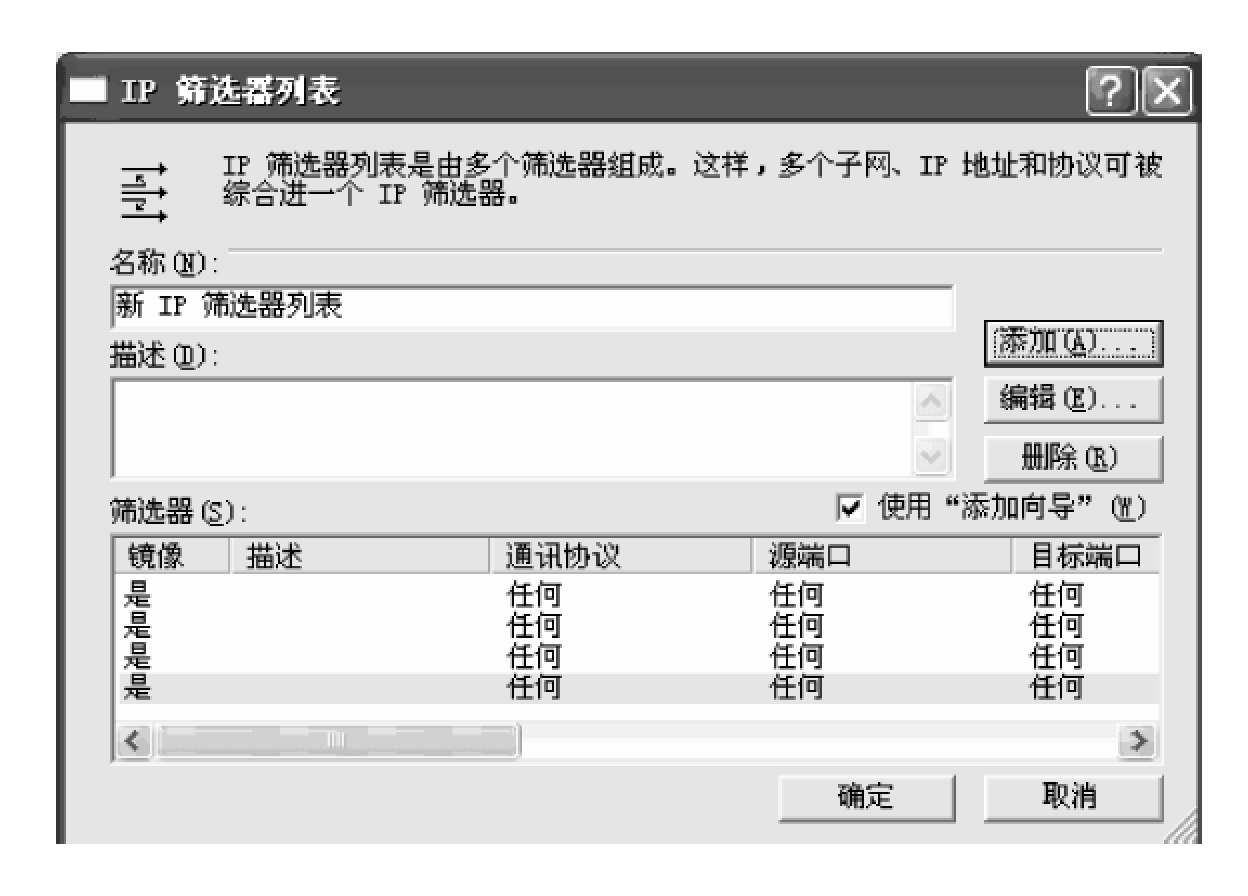


图 5.68　显示添加的筛选器

第 16 步：单击“添加”和“关闭”按钮保存此前的设置，可在“IP 筛选器列表”对话框中看到新建立的名为“新 IP 筛选器列表”的筛选器，如图 5.69 所示。

默认情况下，IP Filter 的作用是单方面的，如发送端用户是 A，接收端用户是 B，则防火墙只对 A→B 的流量起作用，而忽略对 B→A 的流量。若选中 Mirror(双向)，则防火墙对 A→B、B→A 的双向流量都进行处理(相当于一次添加了两条规则)。

此时，在通过本机访问 www.163.com 网站时会收到失败的回应消息，这是因为刚才只是简单建立了过滤规则而没有明确具体信息。在实际使用中明确过滤的源地址、目的地址和使用协议后，就可以使用此方法结合 IPSec 中的 IP Filter 达到防火墙过滤非法数据包的功能。



图 5.69 新 IP 筛选器列表

(3) IP Filter 高级技巧

① 备份设置的过滤规则

如果用户已经建立了很多条过滤规则,那么如何将其保存以备后用或者其他计算机使用呢?实际上操作起来很简单,右击"IP 安全策略,在本地计算机"选项,选择"所有任务"下的"导出策略"选项即可。若在其他计算机上使用"所有任务"下的"导入策略"选项,就可以实现多台计算机快速使用同一个策略的功能,如图 5.70 所示。

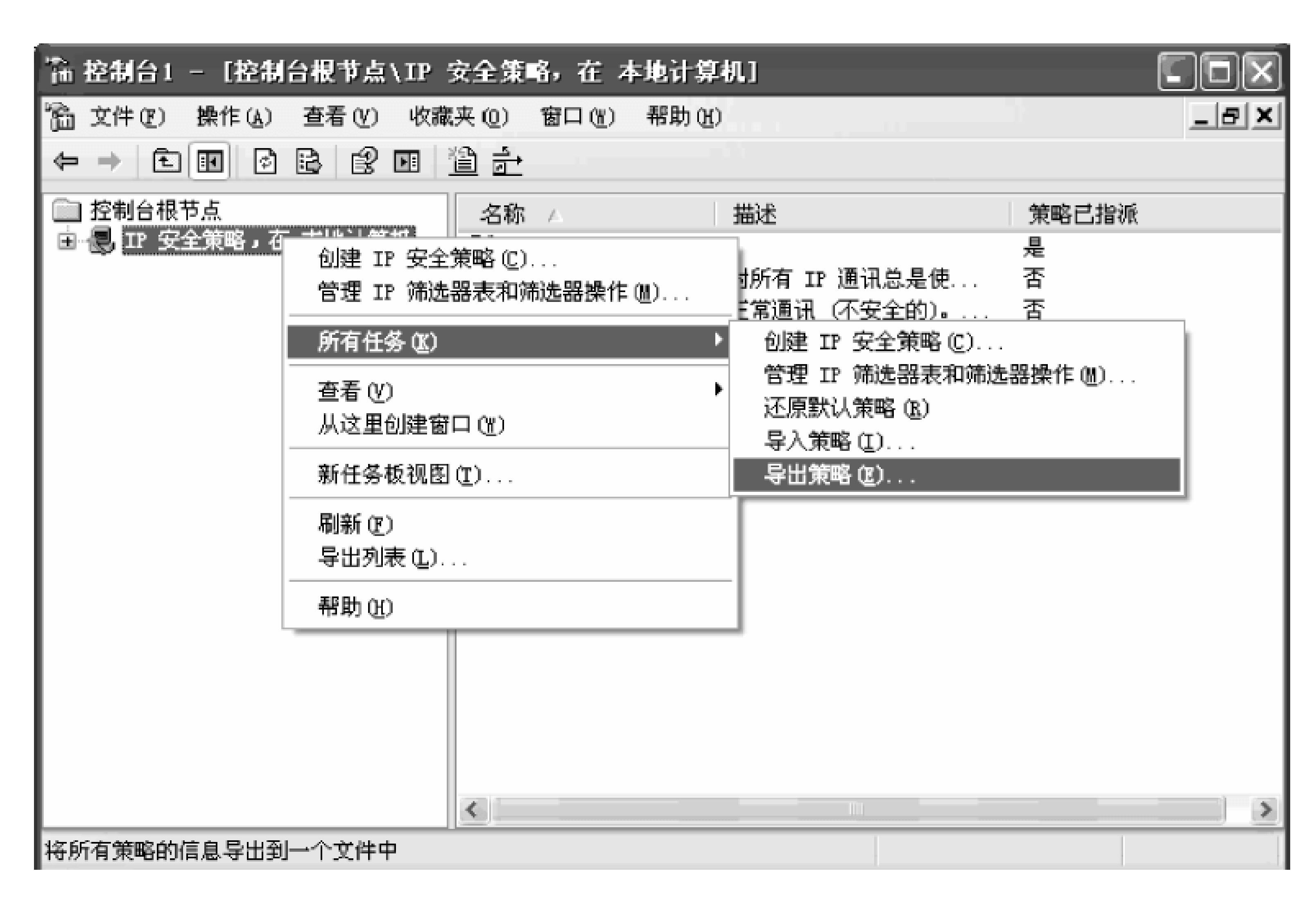


图 5.70 选择"导出策略"

② 单防火墙的多策略

如果用户使用的是笔记本电脑,经常在家中和单位场合交替使用,若是使 IP Filter 单过滤系统拥有多项策略,就方便使用该防火墙系统了。这样,可在家中使用一套过滤方案,

在单位使用另一套过滤方案。

使 IP Filter 单过滤系统拥有多项策略的方法很简单，按照上面介绍的步骤在“IP 筛选器列表”中建立多个筛选器，依次命名为“单位 IPSec 设置”和“家庭 IPSec 设置”。这样就可在不同场所使用不同过滤列表了，如图 5.71 所示。

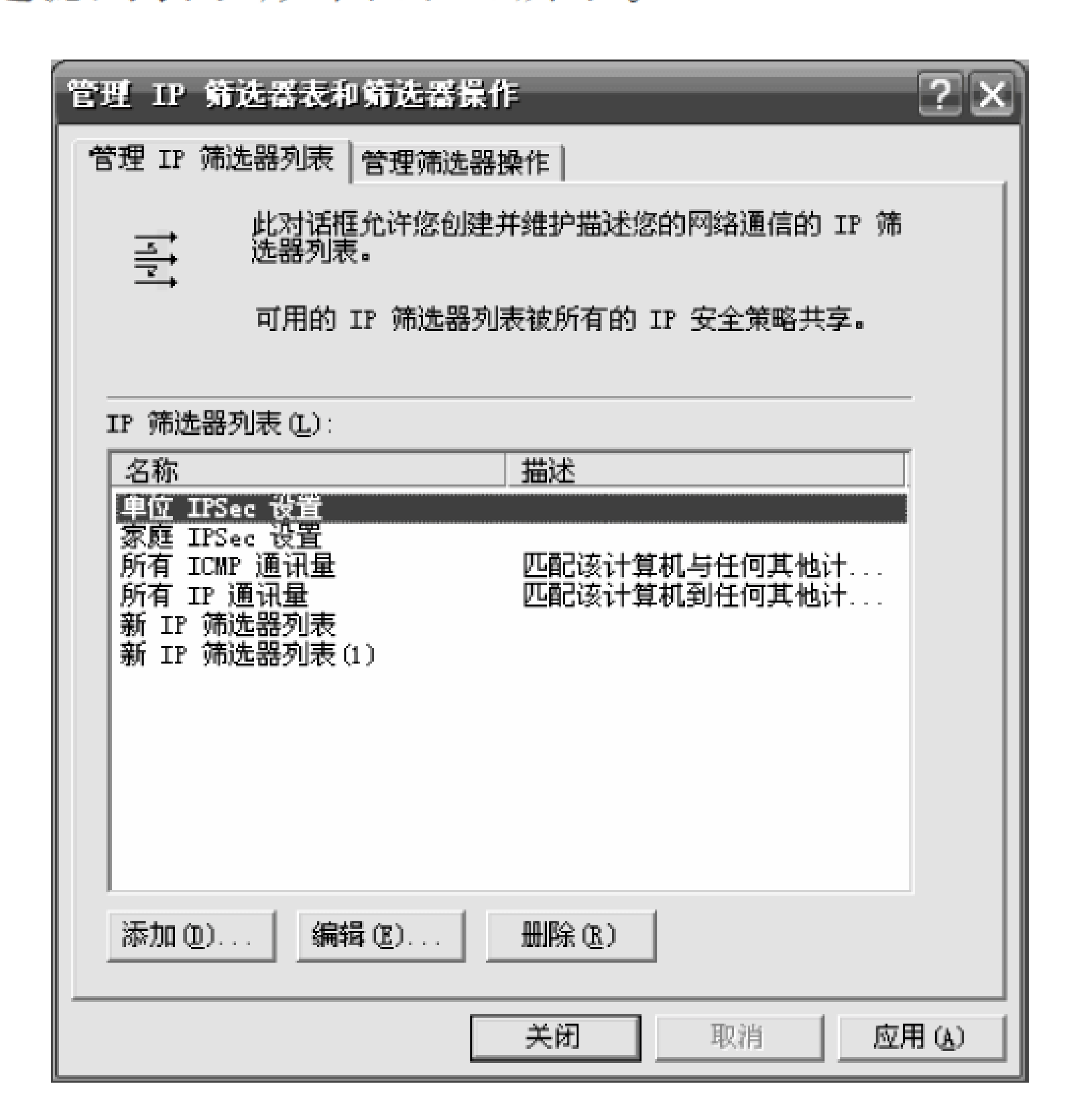


图 5.71　建立多个筛选器

③ 快速还原初始设置

有时在为 IP Filter 添加了一些过滤规则后，发现网络无法使用了，这说明用户添加规则的时候出现了问题。如果一个一个地删除这些过滤规则是可以的，但是太麻烦。IP Filter 有一个默认设置，用户可以通过 IP Filter 中的“恢复默认设置”功能来完成还原初始设置。方法是在“IP 安全策略，在本地计算机”上右击选择“所有任务”下的“还原默认策略”即可。这样原来设置的所有策略都将被清空，如图 5.72 所示。

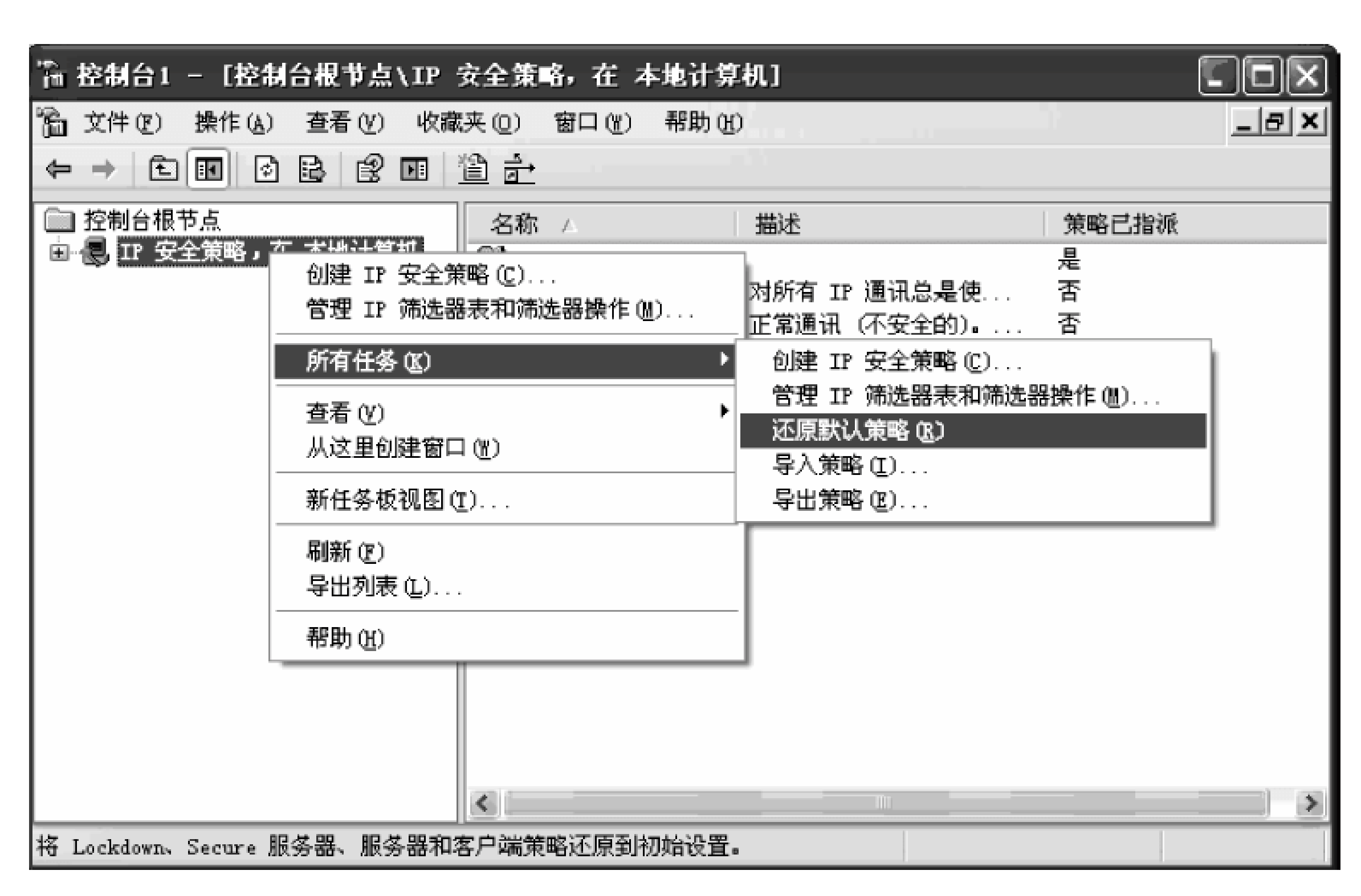


图 5.72　还原默认策略

习题和思考题

一、问答题

1. 简述 TCP/IP 协议的层次结构和主要协议的功能。

2. 简述 EFS 系统的特性。

3. Kerberos 系统主要提供什么服务?

4. IPSec 的主要作用是什么?

二、填空题

1. TCP/IP 协议集由上百个协议组成,其中最著名的协议是(　　)协议和(　　)协议。

2. IP 协议提供(　　)、(　　)和(　　)服务。

3. TCP/IP 的网络接口层安全一般可做到点对点间较强的(　　)、(　　)和连续的信道认证。

4. TCP/IP 协议的网络层提供基于(　　)的安全服务,相应的安全协议可用来在 Internet 上建立安全的(　　)通道和 VPN。

5. TCP/IP 协议的传输层安全机制的主要优点是提供基于(　　)的安全服务。

6. TCP/IP 协议的应用层提供对每个应用(包括应用协议)进行(　　)的安全服务,加入新的安全功能。

7. 已实现的 TCP/IP 应用层安全技术有(　　)、SEPP、(　　)和 S-HTTP 协议等。

8. 加密文件系统(EFS)是 Windows 文件系统内置的(　　),它以(　　)为基础,提供一种透明的(　　)服务。

9. EFS 作为操作系统级的安全服务,当保存文件时 EFS 将自动对文件进行(　　),当用户重新打开文件时系统将对文件进行(　　)。

10. 使用 EFS 加密功能的两个条件分别是(　　)和(　　)。

11. Kerberos 是一种提供(　　)的系统,通过密钥系统为 Client/Server 应用程序提供强大的认证服务。Kerberos 是一种基于(　　)的第三方认证协议。此外,它还能够提供对通信数据的(　　)保护。

12. IP 安全协议(IPSec)是一个网络安全协议标准,其主要功能是为 IP 通信提供(　　),保护 TCP/IP 通信免遭(　　),有效抵御(　　),同时保持其易用性。

13. IPSec 是由(　　)、(　　)、(　　)和用于网络认证及加密的一些算法组成的系列协议。

14. IPSec 可用于 IPv4 和(　　)环境,它有(　　)和(　　)两种工作模式。

15. IPSec 可对数据进行(　　)。AH 协议用于(　　),ESP 协议用于(　　)。

三、单项选择题

1. IPSec 服务可提供(　　)。

A. 非否认服务功能　　B. 证书服务功能

C. 数据完整性服务功能　　D. 加密和认证服务功能

2. EFS 系统可提供(　　)。

A. 认证服务功能　B. 证书服务功能　C. 数据完整性服务　D. 加密服务功能

3. IPSec是由AH、ESP、IKE和用于网络认证及加密的一些算法组成的系列协议。密钥的管理和交换功能是由(　　)提供的。

A. AH　　B. ESP　　C. IKE　　D. PKI

4. 由于IP协议提供无连接的服务,在传送过程中若发生差错就需要(　　)协议向源节点报告差错情况,以便源节点对此做出相应的处理。

A. TCP　　B. UDP　　C. ICMP　　D. RARP

四、实验题

1. 设置软件限制策略实验:利用Gpedit.msc打开组策略编辑器,依次展开"计算机配置"→"Windows设置"→"安全设置"→"软件限制策略"路径,在"操作"菜单选择"创建新的策略"。

2. EFS加密和解密实验:利用EFS功能加密文件/文件夹、解密加密的文件/文件夹、找回EFS加密文件。

3. IPSec实验:利用系统的"本地安全设置"功能进行IP安全策略和规则设置。

第6章 网络攻防技术与应用实践

网络安全系统是一个复杂的系统,它涉及系统安全和风险评估、系统安全策略、安全防护和安全检测技术,以及具体的安全措施。前述各章介绍的网络访问控制、网络实体安全、网络安全管理、操作系统安全、数据备份和加密、数字签名和身份验证等大部分都是安全防护的内容。安全防护可以预防和避免大多数的不安全事件,但不能阻止所有的不安全事件,特别是像病毒和黑客等利用系统缺陷和攻击手段侵入网络系统的恶性事件。一旦病毒或黑客侵入网络系统,网络管理员就要根据入侵事件的特征对系统进行入侵检测;通常也可使用有关软件工具对系统进行安全扫描和监听(或嗅探)。通过对网络系统不断的检测、扫描和监听,可发现入侵者的行为。网络管理员一旦检测和监控到入侵行为,就要采取措施清除入侵的危害和进行恢复处理。

本章将介绍网络病毒、黑客及网络攻击、网络防火墙、入侵检测系统、网络扫描、网络监听(包括嗅探)等网络攻击及防范方面的内容。

6.1 网络病毒与防范

计算机病毒是一种计算机程序,它不仅能破坏计算机系统,而且能将病毒传播、感染其他系统。计算机病毒通常隐藏在其他看起来无害的程序中,能生成自身的复制品并将其插入其他的程序中,执行恶意的行动。

几乎所有的人都听说过"计算机病毒"这个名词。使用过计算机的人大多都领教过计算机病毒的厉害。对网络管理员来说,防御计算机病毒有时是比其他管理更困难的任务。对用户来说,了解和预防计算机病毒的威胁显得格外重要。

任何计算机病毒都是人为制造的、具有一定破坏性的程序。概括起来,计算机病毒具有破坏性、传染性、隐蔽性、潜伏性、不可预见性和针对性等特征。

6.1.1 网络病毒概述

随着 Internet 技术的发展,计算机病毒的含义也在逐步发生变化,与计算机病毒特征和危害有类似之处的特洛伊木马和蠕虫,从广义角度而言也可归为计算机病毒之列。特洛伊木马通常又称为黑客程序,其关键是采用隐藏机制执行非授权操作;蠕虫通过网络来扩散和传播特定的信息或错误,进而造成网络服务遭到拒绝,并出现死锁现象或使系统崩溃,蠕虫对网络系统的危害日益严重。

网络病毒实际上是一个笼统的概念，可以从两方面理解：一是专门指在网络上传播，并对网络进行破坏的病毒；二是指与 Internet 有关的病毒，如 HTML 病毒、电子邮件病毒、Java 病毒等。提起网络病毒，使用网络系统（包括 Internet）的用户想必并不陌生，甚至很多用户深受其害。人们也使用了许多种防病毒软件，但仍经常受到病毒的攻击。

1. 网络病毒的传播

Internet 的开放性为病毒广泛传播提供了方便，Internet 本身的安全漏洞也为产生新的病毒提供了良好条件，加之一些新的网络编程软件（如 Java Script、ActiveX）也为计算机病毒渗透到网络的各个角落提供了便利。

在网络中计算机病毒的入侵点有服务器、电子邮件、BBS 上下载的文件、WWW 站点、FTP 文件下载、网络共享文件及常规的网络通信、盗版软件、示范软件和其他共享设备。Internet 上有众多的软件、工具可供下载，有大量的数据交换，这给病毒的大面积传播提供了可能和方便。Internet 本身也衍生出一些新的病毒，如 Java 和 ActiveX 病毒。这些病毒不需要寄主程序，可通过 Internet 到处肆虐寄主，可以与传统病毒混杂在一起不被人们觉察，更有甚者，它们可跨越操作平台，一旦传染，便可毁坏所有操作系统。网络病毒一旦突破网络安全系统，传播到网络服务器，进而在整个网络上蔓延、再生，就会使网络资源遭到严重破坏。

除通过电子邮件传播外，病毒入侵网络的途径还有：病毒通过工作站传播到服务器硬盘，再由服务器的共享目录传播到其他工作站；网络上下载带病毒的文件的传播；入侵者通过网络漏洞的传播等。

2. 网络病毒的特点

计算机网络的主要功能是资源共享和数据传输。一旦共享资源感染了病毒，网络各节点间信息的频繁传输会将病毒传染到所共享的机器上，从而形成多种共享资源的交叉感染。网络病毒的迅速传播，将造成比单机病毒更大的危害，因此网络环境下计算机病毒的防治就显得更加重要了。

网络环境下的计算机病毒有以下特点。

（1）传播方式复杂，传播速度快、范围广

病毒入侵网络主要是通过电子邮件、网络共享、网页浏览、服务器共享目录等方式，病毒的传播方式多且复杂。在网络环境下病毒可以通过网络通信机制，借助于网络线路进行迅速传输和扩散，特别是通过 Internet，一种新出现的病毒可以迅速传遍全球各地。

（2）破坏危害大

网络病毒将直接影响网络的工作，轻则降低速度，影响工作效率，造成重要数据丢失，重则破坏服务器系统资源，造成网络系统瘫痪，使众多工作毁于一旦，甚至有些信息系统和网络被人为控制。

（3）病毒变种多，病毒功能多样化

利用种类繁多且丰富的编程语言编制的计算机病毒种类繁杂，这些病毒容易编写，也容易修改、升级，从而生成许多新的变种。有些现代病毒有后门程序的功能，这些病毒一旦侵入计算机系统，病毒控制者可以从入侵的系统中窃取信息，进行远程控制。

(4) 清除难度大,难以控制

在网络环境下病毒感染的站点数量多、范围广,只要有一个站点的病毒未清除干净,它就会在网络上再次被传播开来,甚至是刚刚完成清除任务的站点,因此现代病毒的清除工作难度极大;且病毒一旦在网络环境下传播、蔓延,就很难对其进行控制。

3. 网络病毒的预防

由于网络病毒通过网络传播,因此建立网络系统病毒防护体系,采用有效的网络病毒预防措施和技术显得尤为重要。网络管理人员和操作人员要在思想上有防病毒意识,以预防为主。防范网络病毒主要从技术和管理两方面入手。

采取有效、成熟的技术措施预防网络病毒是十分重要的。针对病毒的特点,利用现有的技术和开发新的技术,使防病毒软件在与病毒的抗争中不断得到完善,更好地发挥保护作用。现在已有很多较成熟的防病毒技术和软件系统被广大计算机用户使用。

用户在使用网络系统时也要有严格的管理措施。病毒预防的管理问题,涉及管理制度、行为规章和操作规程等。如计算机机房或网络系统要制定严格的管理制度,避免蓄意制造、传播病毒的事件发生;对接触计算机系统的人员进行选择和审查;对系统工作人员和资源进行访问权限划分;下载的文件要经过严格检查,甚至下载文件、接收邮件要使用专门的终端和账号,接收到的程序要严格限制执行等。通过建立安全管理制度,及早发现和清除安全隐患,可减少或避免计算机病毒的入侵。此外,在管理方面也涉及法律和行政法规、安全宣传和培训等问题。

4. 网络病毒的清除

当网络系统感染病毒后,可采取以下措施进行紧急处理,恢复系统或受损部分。

(1) 隔离

当某计算机感染病毒后,可将其与其他计算机进行隔离,避免相互复制。当网络中某节点感染病毒后,网络管理员必须立即切断该节点与网络的连接,以避免病毒扩散到整个网络。

(2) 报警

病毒感染点被隔离后,要立即向网络系统安全管理人员报警。

(3) 查毒源

接到报警后,系统安全管理人员可使用相应防病毒系统鉴别受感染的机器和用户,检查那些经常引起病毒感染的节点和用户,并查找病毒的来源。

(4) 采取应对方法和对策

网络系统安全管理人员要对病毒的破坏程度进行分析检查,并根据需要决定采取有效的病毒清除方法和对策。如果被感染的大部分是系统文件和应用程序文件,且感染程度较深,则可采取重装系统的方法来清除病毒;如果感染的是关键数据文件,或破坏较严重时,可请防病毒专家进行清除病毒和恢复数据的工作。

(5) 修复前备份数据

在对被感染的病毒进行清除前,尽可能将重要的数据文件备份,以防在使用防毒软件或其他清除工具查杀病毒时,也将重要数据文件误杀。

（6）清除病毒

重要数据备份后，运行查杀病毒软件，并对相关系统进行扫描。发现有病毒，立即清除。如果可执行文件中的病毒不能清除，应将其删除，然后再安装相应的程序。

（7）重启和恢复

病毒被清除后，重新启动计算机，再次用防病毒软件检测系统是否还有病毒，并将被破坏的数据进行恢复。

当确定病毒已侵入系统后，可使用防病毒软件对计算机病毒进行查杀。目前成熟的防病毒软件已经可以做到对所有的已知病毒进行检测和清除，瑞星、诺顿、金山毒霸、KV等防病毒软件均有2010新版问世。

6.1.2　木马和蠕虫

1. 木马

特洛伊木马（简称木马）是根据古希腊神话中的木马来命名的，如今黑客程序借用其名，有“一经潜入，后患无穷”之意。这种程序从表面上看没有什么，但是实际上却隐含着恶意企图。一些木马程序会通过覆盖系统中已有文件的方式存在于系统中，还有一些木马会以软件的身份出现。这种代码通常不容易被发现，因为它一般以一个正常应用的身份在系统中运行。

木马与传统病毒不同。木马是一种带有恶意性质的恶意代码，通常悄悄地在寄宿主机上运行，在用户毫无察觉的情况下让攻击者获得了远程访问和控制系统的权限。它一般是以寻找后门、窃取密码和重要文件为主，还可以对计算机进行跟踪监视、控制、查看、修改资料等操作，具有很强的隐蔽性、突发性和攻击性。

木马的传播方式主要有三种：一种是通过E-mail，控制端将木马程序以附件形式附着在邮件上发送出去，收件人只要打开附件就会感染木马；第二种是软件下载，一些非正式的网站以提供软件下载的名义，将木马捆绑在软件安装程序上，程序下载后只要一运行这些程序，木马就会自动安装；第三种是通过会话软件（如QICQ）进行传播，不知情的网友一旦打开带有木马的文件就会感染木马。

木马也是一种后门程序，它会在用户的计算机系统里打开一个“后门”，黑客就会从这个被打开的特定“后门”进入系统，然后就可以随心所欲摆布用户的计算机了。木马可以读、写、存储和删除文件，可以得到用户的隐私信息和密码，而且还能够控制用户的鼠标和键盘去做他想做的任何事。可以说用户能够在自己的计算机上做什么，木马也同样能做什么。

木马已对用户信息的安全构成了极大隐患，做好木马的防范已经刻不容缓。用户要提高对木马的警惕，尤其是网络游戏玩家更应该提高对木马的关注。

网络中比较流行的木马程序传播速度比较快，影响也比较严重，因此尽管人们掌握了很多木马的检测和清除方法及软件工具，但这些也只是在木马出现后被动的应对措施。当然最好的情况是不出现木马，这就要求大家平时要有对木马的预防意识和措施，做到防患于未然。以下是几种简单适用的木马预防措施。

① 不随意打开来历不明的邮件，阻塞可疑邮件。

② 不随意下载来历不明的软件。

③ 及时修补漏洞和关闭可疑端口。

④ 尽量少用共享文件夹。

⑤ 运行实时监控程序。

⑥ 经常升级系统和更新病毒库。

⑦ 限制使用不必要的、具有传输能力的文件。

可以通过查看系统端口开放的情况、系统服务情况、系统任务运行情况、网卡的工作情况、系统日志及运行速度有无异常等对木马进行检测。可以通过查看在本机上开放的端口，看是否有可疑的程序打开了某个可疑的端口。假如查看到有可疑的程序在利用可疑端口进行连接，则很有可能是感染了木马。可使用 Windows 本身自带的 netstat 命令、Windows 系统下的命令行工具 fport 和图形化界面工具 Active Ports 查看端口。

通过查看系统进程并停止可疑的系统进程，在看到有木马程序运行时，要马上停止系统进程，并进行下一步操作，修改注册表和清除木马文件。

检测到计算机感染木马后，就要根据木马的特征来进行清除。最简单的检测和删除木马的方法是安装木马查杀软件。常用的木马查杀工具(如 KV 3000、瑞星、TheCleaner、木马克星等)都可以进行木马的检测和查杀。

2. 蠕虫

蠕虫是一种可以自我复制的、完全独立的程序，它的传播不需要借助被感染主机的其他程序。蠕虫的自我复制不像其他病毒，它可以自动创建副本，并在没人干涉的情况下自动运行。蠕虫是通过系统中存在的漏洞和设置的不安全性进行入侵的。

蠕虫是一种通过网络传播的恶性代码，它除具有普通病毒的传播性、隐蔽性和破坏性外，还具有一些自己的特征，如不利用文件寄生、可对网络造成拒绝服务、与黑客技术相结合等。蠕虫的传染目标是网络内的所有计算机。网络蠕虫作为对互联网危害严重的一种计算机程序，其破坏力和传染性不容忽视。

局域网条件下的共享文件夹、电子邮件和网络中的恶意网页、大量存在着漏洞的服务器等都成为蠕虫传播的途径。网络的发展也使得蠕虫可以在几个小时内蔓延到全球，而且蠕虫的主动攻击性和突然爆发性将使得人们惊慌失措。

蠕虫具有传播迅速、难以清除、利用操作系统和应用程序的漏洞主动进行攻击、传播方式多样化、与黑客技术结合等特点。

与普通病毒不同的是蠕虫能利用漏洞进行传播和攻击。这里所说的漏洞主要是软件缺陷和人为缺陷。软件缺陷(如远程溢出、微软 IE 和 Outlook 的自动执行漏洞等)需要软件厂商和用户共同配合，不断地升级软件而解决。人为缺陷主要是指计算机用户的疏忽。对于企业用户来说，威胁主要集中在服务器和大型应用软件上；而对个人用户，主要是防范人为缺陷。

企业网络防范蠕虫的一个重要方面就是管理策略，包括加强网络管理员安全管理水平，提高安全技术和安全意识；建立对蠕虫的检测系统，能够在第一时间内检测到网络的异常和蠕虫攻击；建立应急响应系统，将风险减少到最低；建立备份和容灾系统防止意外灾难下的数据丢失。

对于个人用户而言，蠕虫一般采取电子邮件和恶意网页传播方式。通过电子邮件传播

的蠕虫通常利用的是社会工程学欺骗，即以各种各样的欺骗手段诱惑用户点击的方式进行传播。防范此类蠕虫需要用户提高防杀恶意代码的意识；购买正版的防病毒（蠕虫）软件；经常升级病毒库；不随意查看陌生邮件，尤其是带有附件的邮件。

6.1.3　典型防病毒软件应用实例——卡巴斯基软件的应用

1. 卡巴斯基软件简介

现在，杀毒软件已成为计算机中必装软件之一。各个厂家纷纷推出各种杀毒软件产品，国际著名杀毒软件公司或产品有卡巴斯基、诺顿、McAfee 等，国内著名杀毒软件公司或产品有瑞星、江民、金山毒霸等。

现代杀毒软件所采用的查毒、杀毒技术大同小异，工作原理与使用方法基本相同。本节就以市面上流行的国际著名品牌杀毒软件——卡巴斯基（Kaspersky）为例介绍防病毒软件的安装、配置与使用方法。

卡巴斯基软件来源于俄罗斯，是世界上最优秀、最顶级的网络杀毒软件之一。它提供了所有类型病毒的防护功能，如抗病毒扫描、监控、行为阻断和完全检验等。它支持几乎所有的普通操作系统、E-mail 和防火墙。卡巴斯基防病毒软件有许多国际研究机构、中立测试实验室和 IT 出版机构的证书，确认了卡巴斯基具有汇集行业最高水准的突出品质。

卡巴斯基软件目前与安全卫士 360 合作，安装安全卫士 360 后可以获得卡巴斯基半年的使用，也可以到卡巴斯基官方网站下载 30 天试用期的试用版。

卡巴斯基可供免费试用的查毒产品主要有两种：卡巴斯基防病毒软件 6.0 个人版和卡巴斯基互联网安全套装 6.0 个人版，两者区别不大。前者仅提供查杀病毒，后者还提供网络安全功能。

卡巴斯基防病毒软件单机版为家庭用户的个人电脑提供超级病毒防护，它具有最尖端的防病毒技术，时刻监控病毒可能入侵的途径，同时该产品应用独有的 iCheckerTM 技术，使处理速度比同类产品快 3 倍，而且它还应用第二代启发式病毒分析技术识别未知恶意程序代码，成功率约达 100%。卡巴斯基病毒数据库样本数已经超过 10 万种，并拥有世界上最快的升级速度，每小时常规升级一次，以使系统随时保持抗御新病毒侵害的能力。

卡巴斯基软件可以基于 SMTP/POP3 协议来检测进出系统的邮件，可实时扫描各种邮件系统全部接收和发出的邮件，检测其中的所有附件，包括压缩文件和文档、嵌入式 OLE 对象及邮件体本身。它还新增加了个人防火墙模块，可有效保护运行 Windows 操作系统的 PC，探测对端口的扫描、封锁网络攻击并向管理员提出报告，系统可在隐形模式下工作，封锁所有来自外部网络的请求，使用户隐形和安全地在网上遨游。

卡巴斯基软件可检测出上千种以上的压缩格式文件和文档中的病毒，并可清除 ZIP、ARJ、CAB 和 RAR 文件中的病毒。

2. 卡巴斯基的安装

用户在如图 6.1 所示卡巴斯基软件（6.0 个人版）下载专区下载后，可按如下步骤进行安装。

第 1 步：启动卡巴斯基安装程序，跳过欢迎界面，单击“下一步”按钮开始安装。

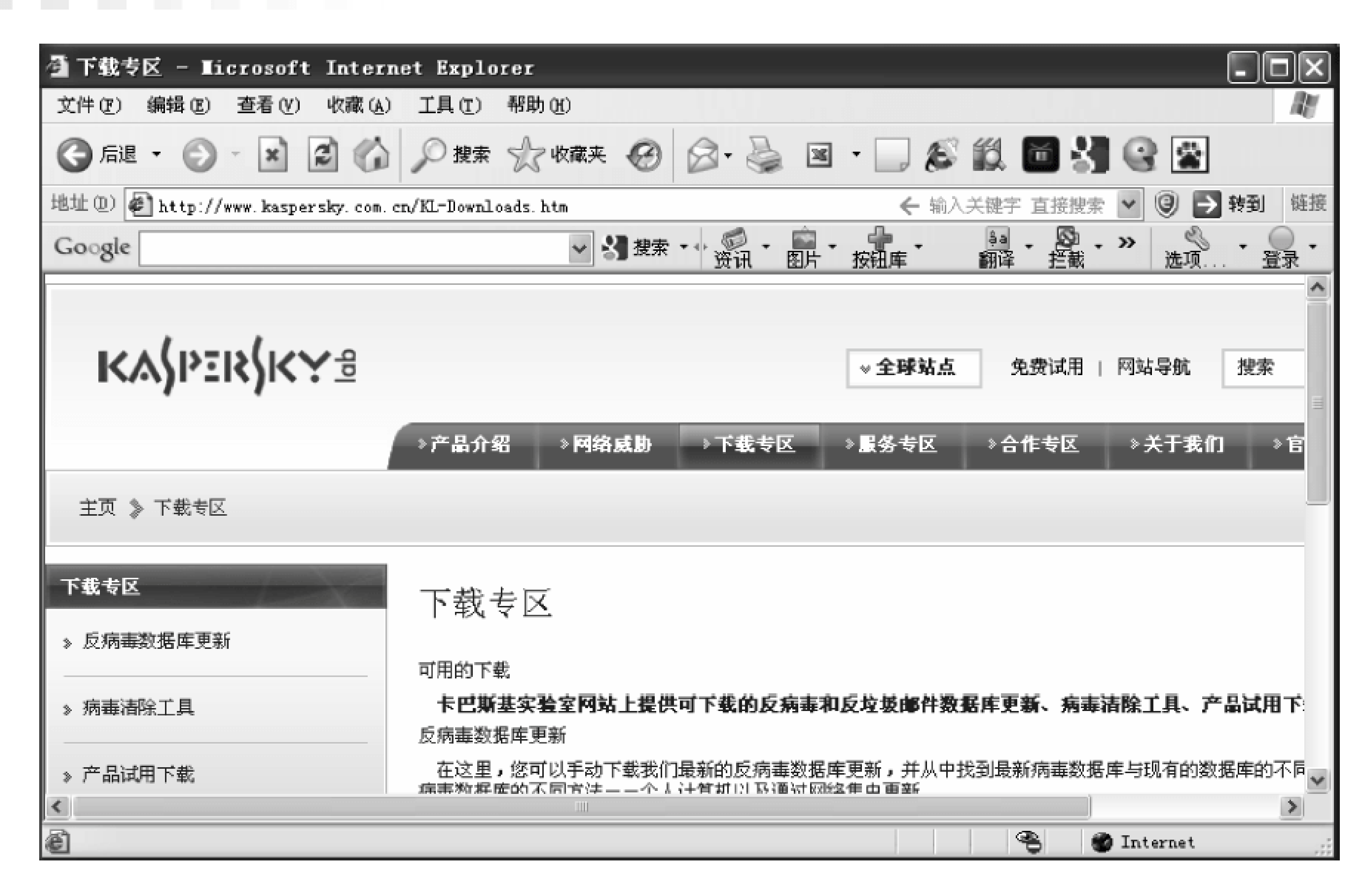


图 6.1　卡巴斯基软件下载专区

第 2 步：认真阅读出现的“终端用户基本许可协议”窗口中的协议后，选中“我接受许可协议条款”单选框，单击“下一步”按钮。

第 3 步：弹出如图 6.2 所示的窗口后，选择安装路径（通常按默认安装路径即可），单击“下一步”按钮。



图 6.2　选择安装路径

第 4 步：在弹出的如图 6.3 所示的窗口中选择安装类型，通常选择“完整”类型，再单击“下一步”按钮。

第 5 步：在弹出的如图 6.4 所示的窗口中选择“启动自我保护”单选框，单击“安装”按钮，开始安装过程。

第 6 步：在弹出的如图 6.5 所示的窗口中，单击“下一步”按钮，完成安装过程。



图 6.3　选择安装类型

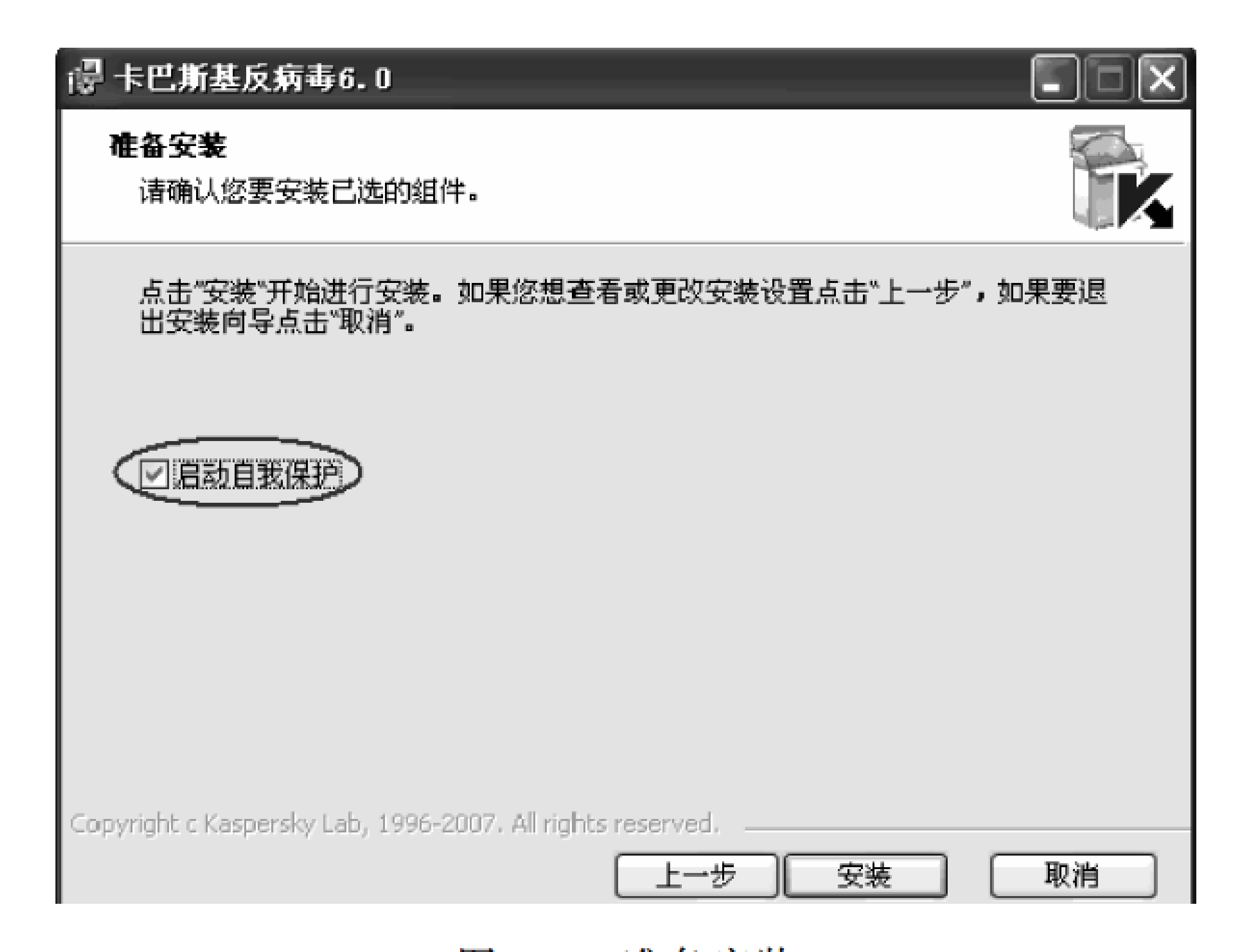


图 6.4　准备安装



图 6.5　安装完成

第 7 步：安装后要进行激活。先选择激活方式，如图 6.6 所示。正式版用户在购买卡巴斯基时会获得一个激活码，此时选中“使用激活码激活”单选钮进行激活，试用版用户可单击“激活试用版”，免费试用 30 天。选择激活方式后单击“下一步”按钮，出现激活成功图示，单击“下一步”按钮即可。



图 6.6　选择激活方式

第 8 步：选择保护方式。如图 6.7 所示，一般选中“基本保护”即可，单击“下一步”按钮，弹出如图 6.8 所示选择病毒特征代码库“更新”窗口，选择“自动”单选框，单击“下一步”按钮。

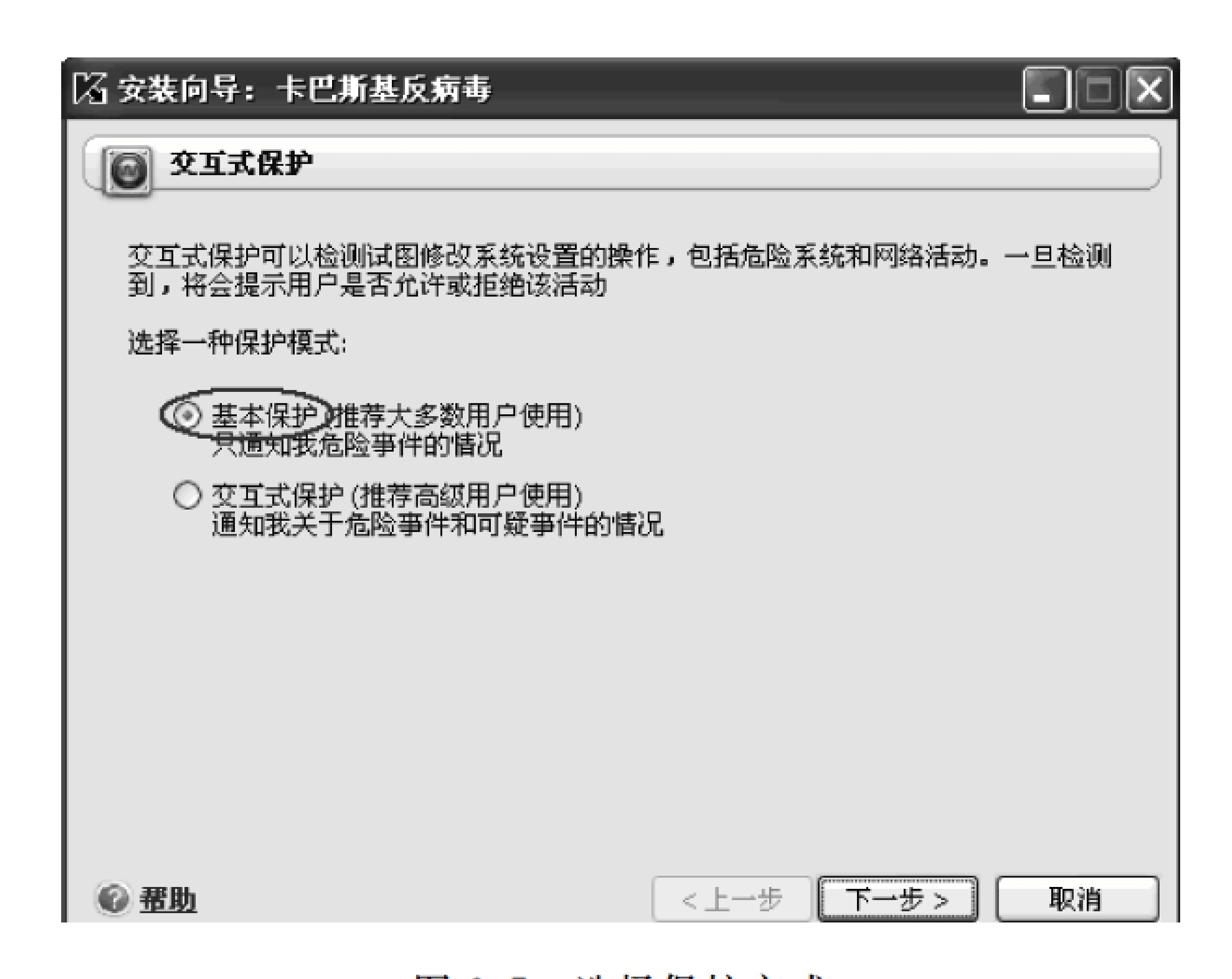


图 6.7　选择保护方式

第 9 步：在选择扫描方式中选择默认值即可，最后完成安装过程。重新启动计算机，卡巴斯基软件即可开始工作。



图 6.8　选择病毒特征代码库“更新”模式

3. 卡巴斯基的配置

安装好卡巴斯基软件后，还需合理配置才能达到最好的效果。合理的配置可以在保证安全的情况下尽量减少对系统资源的占用。

图 6.9 所示为卡巴斯基防病毒软件系统的主界面。单击主界面右上角的“设置”按钮，打开设置窗口，如图 6.10 所示。在左边“设置”栏依次选中不同的对象，在右侧窗格进行配置。



图 6.9　卡巴斯基防病毒软件系统主界面

这里以“文件保护”为例介绍其配置原则与方法。在图左侧窗格选中“文件保护”，在右边窗格单击“自定义”按钮后，弹出如图 6.11 所示的窗口，可在该窗口下进行配置。

(1) 文件类型栏

- “扫描所有文件”选项可靠性最高，但扫描速度最慢。



图 6.10 “设置”窗口



图 6.11 文件保护设置

- “扫描程序及文档”选项依据文件的内容进行有选择性地扫描，对不会被病毒感染的文件不扫描，节省扫描时间，推荐选用此选项。
- “扫描程序和文档”选项根据文件扩展名进行扫描，速度最快，但有可能会有漏扫。

(2) 增量扫描技术栏

选择该项后，卡巴斯基系统可记住此次扫描过的文件，下次再扫描时对于没有改变过的文件不再进行扫描，这样可大大提高查毒速度。

(3) 复合文件栏

对过大的压缩包可以不扫描。因为扫描压缩包时系统会在一个虚拟的计算机中把压缩包打开逐一扫描，耗费了大量的系统资源。而通常压缩包内的程序和文档需要解压缩后才

能使用，此时可再用杀毒软件检查数据包的内容即可。因此可选择“不处理过大的压缩文件”、“如果压缩文件过大则在后台扫描”和“扫描嵌入式 OLE 对象”。

4. 卡巴斯基软件应用实例

利用卡巴斯基防病毒软件查杀病毒的过程如下：

第 1 步：打开卡巴斯基系统(6.0 个人版)，系统主界面如图 6.9 所示。

第 2 步：主界面左侧有一个扫描选项，点选它之后会出现三个选项，卡巴斯基按照扫描的范围不同分为“关键区域”、“我的电脑”和“启动对象”三个扫描区域，如图 6.12 所示。可以根据扫描范围的不同，选择相应的选项进行操作。



图 6.12　卡巴斯基扫描病毒区域

第 3 步：单击“关键区域”，可以看到如图 6.13 所示的中间区域。这是根据不同的要求变化扫描的具体内容，如全部选择或部分选择系统内存、启动对象、引导扇区、system32 等范围。



图 6.13　卡巴斯基扫描的关键区域

第 4 步：单击图 6.13 右下方的“扫描”按钮可进行扫描杀毒。扫描结束后，单击“关闭”按钮，完成此次扫描和查杀，可查看到扫描结果。

第 5 步：当用户只想扫描计算机的内存和引导区范围是否有病毒侵害时，可以选择单击扫描“启动对象”，如图 6.14 所示。这时中间区域会出现“系统内存”、“启动对象”和“引导扇区”三个选择对象。用户可以根据需要进行全部选择或部分选择设置。

第 6 步：单击图 6.14 右侧的“扫描”按钮进行扫描和查杀。



图 6.14　设定“启动对象”扫描区域

第 7 步：扫描查杀后单击“关闭”按钮，可看到扫描“启动对象”过程完成及扫描结果。

说明：扫描查杀“关键区域”和“启动对象”只是对计算机内存、引导区或开机后抢占进程的病毒的扫描措施，它查杀病毒或恶意程序的范围比较小。如果需要全面查杀病毒，则选择“我的电脑”区域并进行扫描查杀。

第 8 步：单击图 6.9 左侧“扫描”项下的“我的电脑”，弹出如图 6.15 所示界面。图中间区域有多项扫描范围，用户可根据需要全部或部分选择。然后单击右侧的“扫描”按钮进行扫描查杀。图 6.16 所示为扫描进行中状态。当扫描到病毒后，单击“全部处理”按钮进行查杀。



图 6.15　设定“我的电脑”扫描区域

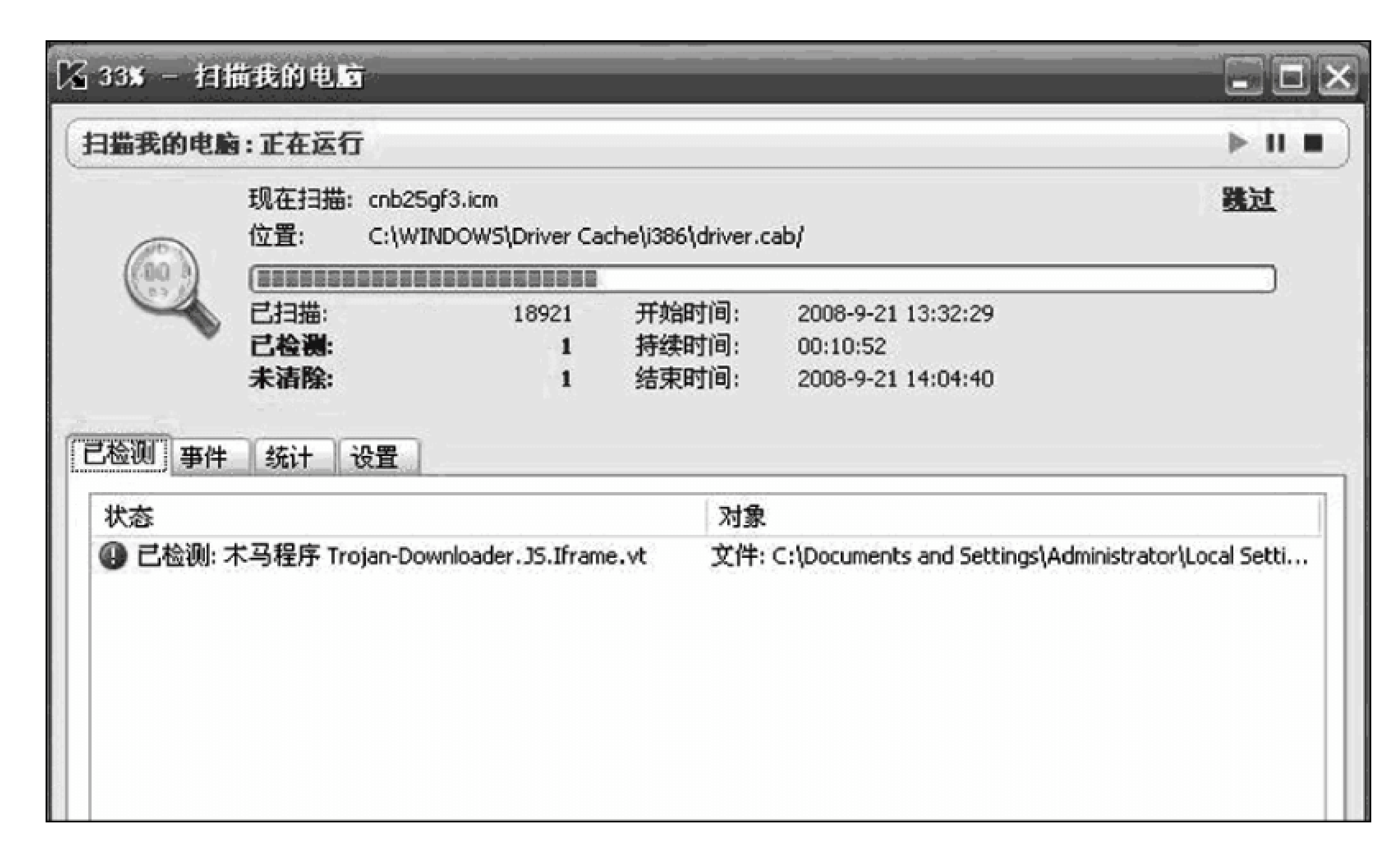


图 6.16 “我的电脑”的扫描过程

第 9 步：查杀完毕后，单击“关闭”按钮退出，界面上会出现扫描“我的电脑”的处理结果。

至此，使用卡巴斯基防病毒工具查杀病毒的过程就全部完成了。

6.2 黑客攻击与防范

提起黑客，总是给人一种神秘莫测的感觉。在人们眼中，黑客是一群精通计算机操作系统和编程语言方面的技术，具有硬件和软件的高级知识，能发现系统中存在安全漏洞的人。在网络中，他们经常使用入侵计算机系统的基本技巧，如破解口令(password cracking)、走后门(backdoor)、安放木马等。他们通常先确定目标并且收集相关信息(包括邮件地址、相关 IP 地址、漏洞等)，然后根据得到的信息进行渗透，未经允许地侵入他人的计算机系统，窥视他人的隐私、窃取密码或故意破坏他人系统，这就是黑客入侵。

6.2.1 黑客与网络攻击

1. 黑客攻击的手段和工具

为了把损失降到最低限度，人们一定要有安全观念，并掌握一定的安全防范措施，让黑客无任何机会可乘。先来了解和研究一下黑客的攻击手段，这样才能采取准确的对策对付网络攻击。

黑客常用的攻击手段有获取用户口令、放置木马程序、电子邮件攻击、网络监听、利用账号进行攻击、获取超级用户权限等。

黑客攻击系统通常使用的工具有扫描器、嗅探器、木马和炸弹等。扫描器是检测本地或远程系统安全脆弱性的软件，利用它通过与目标主机的 TCP/IP 端口建立连接并请求某些服务，记录目标主机的应答，收集目标主机的相关信息，从而发现目标主机某些内在的安全

弱点。嗅探器是一种常用的收集有用数据的工具,利用它可收集用户的账号和密码,或是一些商业性机密数据。著名的木马工具软件,如冰河、BO2000、NetSpy、广外女生等,功能都很强大,黑客广泛利用。被黑客常用的炸弹工具有邮件类炸弹、IP类炸弹和ICQ类炸弹等。

2. 黑客攻击的过程

黑客攻击网络主要有以下过程。

(1) 确定攻击目的

攻击者在进行一次完整的攻击之前,首先要确定攻击要达到的目的,即要给对方造成什么伤害。常见的攻击目的就是破坏和入侵。破坏型攻击就是破坏攻击目标,使其不能正常工作,而不随意控制目标的系统运行。要达到破坏性攻击的目的,主要手段是拒绝服务(DoS)攻击。

(2) 收集信息

黑客在确定攻击目的后,还需进一步获取有关信息,如攻击目标机的IP地址、所在网络的操作系统类型和版本、系统管理人员的邮件地址等,根据这些信息进行分析,可得到有关被攻击方系统中可能存在的漏洞。

(3) 系统安全弱点的探测

在收集到攻击目标的一些信息后,黑客会探测目标网络上的每台主机,以寻求该系统的安全漏洞或安全弱点,黑客主要使用自编程序和利用扫描工具方式进行系统安全弱点的探测。

(4) 建立模拟环境,进行模拟攻击

黑客根据前几步所获得的信息,建立一个类似攻击对象的模拟环境,然后对模拟目标机进行一系列的攻击。在此期间,通过检查被攻击方的日志,观察检测工具对攻击的反应等,可以了解攻击过程中留下的“痕迹”及被攻击方的状态,这样攻击者就知道需要删除哪些文件来毁灭其入侵证据,以此可制定一个系统的、周密的攻击策略。

(5) 实施网络攻击

黑客以前几步所做工作为基础,再结合自身的水平及经验总结出相应的攻击方法,在进行模拟攻击的实践后,将等待时机,实施真正的网络攻击。

通常,黑客实施的网络攻击可能包括以下操作。

① 通过猜测程序可对截获的用户账号和口令进行破译。

② 利用破译程序可对截获的系统密码文件进行破译。

③ 通过得到的用户口令和系统密码远程登录网络,以此获得用户的工作权限。

④ 利用本地漏洞获取管理员权限。

⑤ 利用网络和系统本身的薄弱环节和安全漏洞实施电子引诱(如安放木马)等。

⑥ 修改网页进行恶作剧,或破坏系统程序,或放置病毒使系统陷入瘫痪,或窃取政治、军事、商业秘密,或进行电子邮件骚扰,或转移资金账户、窃取金钱等。

6.2.2 常见的网络攻击类型与防范

对于网络协议、操作系统、数据库和应用程序,无论是其本身的设计缺陷,还是由于人为因素造成的各种漏洞,都可能被黑客利用来进行网络攻击。

1. 黑客的攻击类型

任何以干扰、破坏网络系统为目的的非授权行为都被称为网络攻击。黑客进行的网络攻击通常可归纳为拒绝服务型攻击、利用型攻击和信息收集型攻击。

(1) 拒绝服务型攻击

拒绝服务(DoS)攻击是攻击者通过各种手段来消耗网络带宽或服务器的系统资源,最终导致被攻击服务器资源耗尽或系统崩溃而无法提供正常的网络服务。这种攻击对服务器来说,可能并没有造成损害,但可以使人们对被攻击服务器所提供服务的信任度下降,影响公司声誉以及用户对网络的使用。黑客也会利用 TCP 协议自身的漏洞进行攻击,影响网络中运行的绝大多数服务器。

具体的 DoS 攻击方式有 SYN Flood(洪泛)攻击、IP 碎片攻击、Smurf 攻击、死亡之 ping 攻击、泪滴(teardrop)攻击、UDP Flood(UDP 洪泛)攻击和 Fraggle 攻击等。

(2) 利用型攻击

利用型攻击是一类试图直接对用户机器进行控制的攻击。最常见的利用型攻击有以下 3 种。

① 口令猜测

一旦黑客识别了一台主机而且发现了基于 NetBIOS、Telnet 或 NFS 服务的可利用的用户账号,成功的口令猜测能提供对机器的控制。

② 特洛伊木马

木马是一种直接由黑客或通过用户秘密安装到目标系统的程序。木马一旦安装成功并取得管理员权限,黑客可以直接远程控制目标系统。

③ 缓冲区溢出

由于在很多服务程序中程序员使用类似 strcpy()、strcat()等不进行有效位检查的函数,最终可能导致恶意用户编写一小段程序来进一步打开安全缺口,然后将该代码缀在缓冲区中的有效载荷末尾。当发生缓冲区溢出时,返回指针指向恶意代码,这样系统的控制权就会被夺取。

(3) 信息收集型攻击

信息收集型攻击被用来为进一步入侵系统提供有用的信息。这类攻击主要利用扫描技术和信息服务技术进行,其具体实现方式有地址扫描、端口扫描、反向映射、DNS 域转换和 Finger 服务等。

2. 拒绝服务(DoS)攻击与防范

DoS 攻击主要是攻击者利用 TCP/IP 协议本身的漏洞或网络中操作系统漏洞实现的。攻击者通过发送大量无效的请求数据包造成服务器进程无法短期释放,大量积累耗尽系统资源,使得服务器无法对正常请求进行响应,造成服务器瘫痪。这种攻击主要是用来攻击域名服务器、路由器以及其他网络操作服务。

在 DoS 攻击中,攻击者加载过多的服务将系统资源(如 CPU 时间、磁盘空间、打印机等)全部或部分占用,使得没有多余资源供其他用户使用。由于 DoS 攻击工具的技术要求不高,效果却比较明显,因此成为黑客常用的一种十分流行的攻击手段。

众所周知,在 TCP/IP 传输层,TCP 连接的建立要通过 3 次握手机制完成。客户端首先发送 SYN 信息(第 1 次握手),服务器发回 SYN/ACK 信息(第 2 次握手),客户端连接后再发回 ACK 信息(第 3 次握手),此时连接建立完成。若客户端不发回 ACK,则服务器在超时后处理其他连接。

TCP 的 3 次握手过程常常被黑客利用进行 DoS 攻击,其原理是:客户机先进行第 1 次握手;服务器收到信息后进行第 2 次握手;正常情况下客户机应该进行第 3 次握手。但因为被黑客控制的客户端在进行第 1 次握手时修改了自己的地址,即将一个实际上不存在的 IP 地址填充在自己的 IP 数据包的发送栏中。由于服务器发送的第 2 次握手信息没人接收,所以服务器不会收到第 3 次握手的确认信号,这样,服务器端会一直等待直至超时。当有大量的客户发出请求后,服务器就会有大量的信息在排队等待,直到所有的资源被用光而不能再接收客户机的请求。当正常的用户向服务器发出请求时,由于没有了资源就会被拒绝服务。

可采用防火墙系统、入侵检测系统(IDS)和入侵防护系统(IPS)等技术措施防范 DoS 攻击。此外,从网络的全局着眼,在网间基础设施的各个层面上采取应对措施,如在局域网层面上采用特殊措施、在网络传输层面上进行必要的安全设置,并安装专门的 DoS 识别和预防工具,提供有效的识别机制和强硬的控制手段,这样才能最大限度地减少 DoS 攻击所造成的损失。

对于 DoS 攻击,可采取如下具体措施。

① 关掉可能产生无限序列的服务可防止信息淹没攻击。

② 要防止 SYN 数据段攻击,应对系统设定相应的内核参数,使得系统强制对超时的 SYN 请求连接数据包复位,同时通过缩短超时常数和加长等候队列使得系统能迅速处理无效的 SYN 请求数据包。

③ 建议在该网段的路由器上做些诸如限制 SYN 半开数据包流量和个数配置的调整。

④ 建议在路由器的前端做必要的 TCP 拦截,使得只有完成 TCP 3 次握手过程的数据包才可进入该网段。

对于正在实施的 DoS 攻击,只有追根溯源去找到正在进行攻击的机器和攻击者。要追踪攻击者不是一件容易的事情,一旦其停止了攻击行为就很难被发现。唯一可行的方法就是在其进行攻击的时候,根据路由器的信息和攻击数据包的特征,采用逐级回溯的方法来查找其攻击源头。

3. 分布式拒绝服务(DDoS)攻击与防范

随着 Internet 的发展,出现了越来越多对网络体系进行故意破坏的黑客团体。他们研究出了各种攻击方法,其中最难防范的且最具破坏性的攻击是分布式拒绝服务(DDoS)攻击。DDoS 是一种特殊形式的拒绝服务攻击,采用一种分布、协作的大规模攻击方式,主要目标是商业公司、搜索引擎和政府部门网站等较大站点。DDoS 攻击是黑客经常采用而难以防范的攻击手段。

(1) DDoS 攻击的概念与过程

DDoS 攻击是在传统的 DoS 攻击基础之上产生的一种攻击方式。试想如果计算机与网络的处理能力加大 10 倍,用一台攻击机来攻击不会起作用,但攻击者要是用 10 台、100 台攻击机同时攻击呢? 这就是 DDoS 攻击的思路,它就是利用更多的被控制机发起进攻,以比从前更大的规模来进攻受害者。如图 6.17 所示,为完成 DDoS 攻击,黑客首先要拥有和控

制 3 种类型的计算机：攻击者计算机(黑客本人使用，黑客通过它发布实施 DDoS 的指令)、控制傀儡机(一般不属黑客所有，黑客在这些计算机上安装特定的主控制软件)和攻击傀儡机。每个攻击傀儡机也是一台已被入侵并运行代理程序的系统主机，每个响应攻击命令的攻击傀儡机会向被攻击目标主机发送 DoS 数据包。

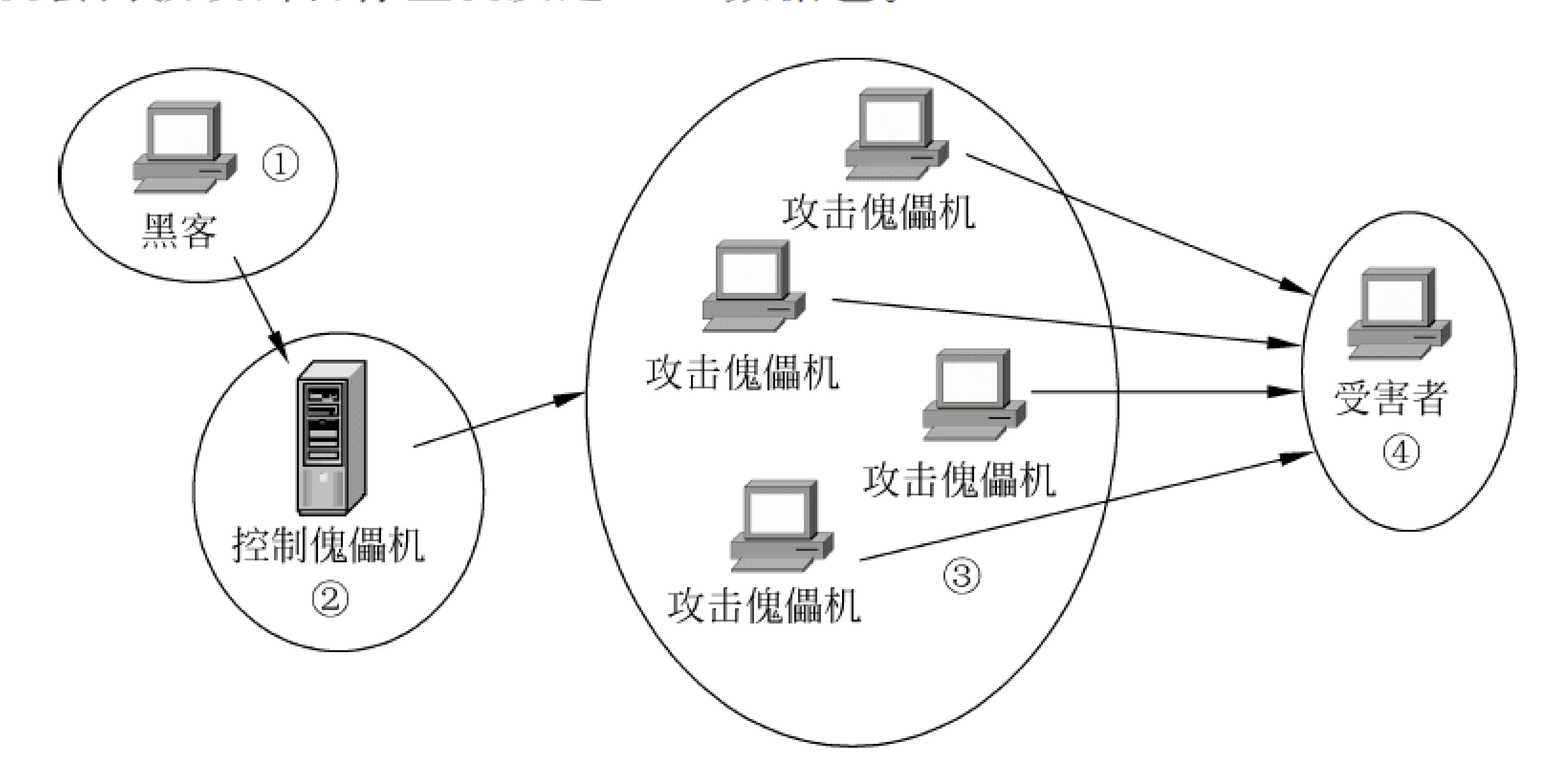


图 6.17　分布式拒绝服务攻击示意图

DDoS 攻击包是从攻击傀儡机上发出的，控制傀儡机只发布命令而不参与实际的攻击。黑客对这两类计算机有控制权或部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令。平时攻击傀儡机并没有什么异常，只是一旦被黑客控制并接收到指令，它们就成为攻击者了。

一般来说，黑客的 DDoS 攻击分为准备、占领傀儡机、植入程序、实施攻击 4 个阶段。

① 在准备阶段，黑客主要进行搜集和了解目标的情况(如目标主机数目、地址、配置、性能和带宽)。该阶段对于黑客来说非常重要，因为完全了解目标的情况，才能有效地进行攻击。对于 DDoS 攻击者，要攻击某个站点，首先要确定到底有多少台主机在支持这个站点，一个大的网站可能有很多台主机利用负载均衡技术提供同一个网站的 WWW 服务。

② 占领傀儡机阶段实际上是使用了利用型攻击手段。简单地说，就是占领和控制傀儡机，取得最高的管理权限，或至少得到一个有权完成 DDoS 攻击任务的账号。

③ 植入程序阶段是在黑客占领傀儡机后，在控制傀儡机上安装主控制软件；在攻击傀儡机上安装守护程序。攻击傀儡机上的代理程序在指定端口上监听来自控制傀儡机发送的攻击命令，而控制傀儡机接受从攻击者计算机发送的指令。

④ 实施攻击阶段是在前三个阶段基础上，黑客开始瞄准目标准备攻击。黑客登录到控制傀儡机，向所有的攻击机发出攻击命令。这时候潜伏在攻击机中的 DDoS 攻击程序就会响应控制台的命令，一起向受害主机高速发送大量的数据包，导致受害者死机或是无法响应正常的请求。

(2) DDoS 攻击的防范

对 DDoS 攻击的防御可以从对主机与网络两个角度进行安全设置。

① 在主机上可使用网络和主机扫描工具检测脆弱性、采用 NIDS 和嗅探器、及时更新系统补丁等措施防范 DDoS。

② 在网络的防火墙上可以采取禁止对主机的非开放服务的访问、限制同时打开的

SYN 最大连接数、限制特定 IP 地址的访问、严格限制开放服务器的对外访问等设置；在网络路由器上采取检查每一个经过路由器的数据包、设置 SYN 数据包流量速率、在边界路由器上部署策略、使用 CAR 限制 ICMP 数据包流量速率等设置。

4. 缓冲区溢出攻击与防范

(1) 缓冲区溢出及攻击

缓冲区是用户为程序运行时在计算机中申请的一段连续的内存，它保存给定类型的数据。缓冲区溢出是指通过向程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他的指令。缓冲区溢出攻击是一种常见且危害很大的系统攻击手段，这种攻击可以使一个匿名的 Internet 用户有机会获得一台主机的部分或全部控制权。

著名的"莫里斯"蠕虫就利用 UNIX fingered 程序不限制输入长度的漏洞，输入 512 个字符后使缓冲区溢出。该蠕虫程序以 root(根)身份运行，并感染到其他机器上。Slammer 蠕虫也是利用未及时更新补丁的 MS SQL Server 数据库漏洞，采用不正确的方式将数据发到 MS SQL Server 的监听端口，这个错误可以引起缓冲区溢出攻击；攻击代码通过缓冲溢出获得非法权限后，被攻击主机上的 SQLserver.exe 进程尝试向随机的 IP 地址不断发送攻击代码，感染其他机器，最终形成 UDP Flood，造成网络堵塞甚至瘫痪。

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序功能，使攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。为了达到这个目的，攻击者一是要在程序的地址空间里安排适当的代码，二是要适当地初始化寄存器和存储器，让程序跳转到事先安排的地址去执行。因此采用在程序的地址空间里安排适当的代码、控制程序的执行流程使之跳转到攻击代码、综合代码植入和流程控制方法实现缓冲区溢出攻击。

(2) 缓冲区溢出攻击的防范

缓冲区溢出攻击主要利用了 C 程序中数组边境条件、函数指针等设计不当的漏洞，大多数 Windows、Linux、UNIX 和数据库系列的开发都依赖于 C 语言，而 C 语言的缺点是缺乏类型安全。

缓冲区溢出易于实现且危害严重，给系统的安全带来了极大的隐患。防火墙对这种攻击方式无能为力，因为攻击者传输的数据分组并无异常特征，没有任何欺骗。另外可以用来实施缓冲区溢出攻击的字符串非常多样化，无法与正常数据进行有效区分。缓冲区溢出攻击不是一种窃密和欺骗手段，而是从计算机系统的最底层发起的攻击，在它的攻击下系统的身份验证和访问权限等安全策略形同虚设。

可以采用以下几种基本的方法防范缓冲区溢出攻击。

① 编写正确的代码

可利用一些工具和技术来帮助程序员编写安全正确的程序，如编程人员可以使用具有类型安全的语言 Java 以避免 C 语言的缺陷；在 C 语言开发环境下编程应避免使用 Gets、Sprintf 等未限定边境溢出的危险函数；使用检查堆栈溢出的编译器(如 Compaq C 编译器)等。

② 非执行缓冲区保护

通过使被攻击程序的数据段地址空间不可执行，从而使攻击者不可能植入缓冲区的代

码，这就是非执行缓冲区保护。

③ 数组边界检查

这种检查可防止缓冲区溢出的产生。为了实现数组边界检查，所有对数组的读写操作都应当被检查，以确保在正确的范围内对数组的操作。最直接的方法是检查所有的数组操作，但是通常可以采用一些优化的技术来减少检查的次数。

④ 程序指针完整性检查

这种检查可在程序指针被引用之前检测到它的改变。因此，即便一个攻击者成功地改变了程序的指针，由于系统事先检测到了指针的改变，这个指针就不会被使用。

此外，在产品发布前仍需要仔细检查程序溢出情况，将威胁降至最低。作为普通用户或系统管理员，应及时为自己的操作系统和应用程序更新补丁，以修补公开的漏洞，减少不必要的开放服务端口，合理配置自己的系统。

6.2.3　密码保护技巧

利用密码设置和管理漏洞进行攻击是多数黑客常用的方法。攻击者首先是寻找系统是否存在没有密码的账户；其次是试探系统是否有容易猜出的密码，尝试登录；三是使用密码破译一类的工具破解。而存放密码的文件往往是攻击者首先寻找的目标。

大部分用户密码被盗多是因为缺少网络安全保护意识以及自我保护意识，以致被黑客盗取密码后造成重大的损失。现介绍几例密码安全和保护技巧，以飨读者。

1. 密码的设置

用穷举法破解简单且位数较少的密码是有效的。但是如果网络用户把密码设得较长，而且没有明显的规律特征（如用一些特殊字符和数字字母组合），那么用穷举法破解就变得非常困难，这样可提高密码的安全性。

对系统用户而言，不设置密码（空密码）或设置的密码与用户名相同都是很危险的。一般情况下，密码长度应不少于 6 位，密码中最好包含大小写字符、数字、标点符号、控制字符和空格，且这些符号交叉混合排序。用纯数字、姓名拼音、昵称、出生日期、车牌号码、电话号码、常用证件号码、公司名或部门名，或其他很容易想到的相关信息（如常用词、简单英文单词或组合、软件名、计算机名和地名等）作为密码都是很不安全的，应加以避免。不要使用 111111、aaaaaa 等简单数字/字符的重叠组合和连续数字或顺序字母（如 654321、abcdef 等）作为密码。

2. 密码的管理原则

要保持严格的密码管理观念，要定期更换密码（如每月或每季更换一次）；不要保存密码在本地，很多应用软件（如某些 FTP 等）保存的密码并不是设计得非常安全，如果本地没有一个很好的加密策略，那将为黑客破解密码提供了方便；也不要将密码写在笔记本、台历、纸巾、别人可打开的文件中或其他较明显的媒体上。不要重复使用同一密码，也不要交替使用两个密码；不要让人看见自己在输入密码，更不能将密码告诉他人。

对于不同的网络系统应设置不同的密码，对于重要的系统应使用更为安全的密码，不要所有系统使用同一个密码。对于那些偶尔登录的论坛，可以设置简单的密码；对于重要的

信息、电子邮件、网上银行等，必须设置较复杂的密码；如果实在需要，还可以将密码“加密”后保存。

3. 使用软键盘

通过软键盘输入密码是比较容易操作的，是目前对付木马记录击键的有效方法。软键盘也叫虚拟键盘，用户在输入密码时，先打开软键盘，然后用鼠标选择相应的字母输入，这样就可以避免木马记录击键。另外，为了更进一步保护密码，用户还可以打乱输入密码的顺序，这样就可进一步增加黑客破解密码的难度。

为了防止计算机中可能有木马窃取重要的信息，建议在输入用户名或卡号时采取剪切/重排方式：如用户名或卡号为“123456789”，输入时先输入“567891234”，再利用“剪切”加“复制”功能改为正确的号码。这样，记录键盘操作的木马也就无法取得正确的用户名或卡号了。

4. 使用动态密码

动态密码(dynamic password)也称一次性密码，它是指用户的密码按照时间或使用次数不断地动态变化，每个密码只使用一次。动态密码对于截屏破解非常有效，因为即使截屏破解了密码，也仅仅破解了一个密码，下一次登录时不会再使用这个密码。

基于硬件技术的动态密码锁采用一种称为动态令牌的专用硬件。该硬件内置电源、密码生成芯片和显示屏，使用该硬件可以产生动态的一次性密码。该密码锁在使用前必须输入静态的 PIN 码才能进入产生密码，只有持有密码锁且知道 PIN 码的用户才能产生动态密码。采用硬件的不可复制特性，使得密码的产生与终端分离，安全性高于软件方式。由于每次使用的密码必须由动态令牌来产生，而用户每次使用的密码都不相同，因此黑客很难计算出下一次出现的动态密码，增强了安全性。

5. 生物特征识别

生物特征识别技术指通过计算机，利用人体所固有的生理特征或行为特征来进行个人身份鉴定。常用的生物特征有指纹、掌纹、视网膜、声音、笔迹、脸像等。生物特征识别是一种简单可靠的生物密码技术，该技术认定的是人本身。由于每个人的生物特征具有与其他人不同的唯一性，以及在一定时期内不变的稳定性，不易被伪造和假冒。因此，建议用户在条件允许的情况下，采用生物特征密码技术进行识别。目前，在人体特征识别技术市场上，占有率最高的是指纹机和手形机，这两种识别方式也是目前最成熟的技术。

6.3 网络防火墙安全

Internet 的迅速发展给现代人的生产和生活都带来了前所未有的影响，大大提高了工作效率，丰富了人们的精神和文化生活。但由于 Internet 是一个开放式的全球性网络，其结构错综复杂，网上的浏览访问不仅使数据传输量增加，网络被攻击的可能性也增大。因此，网络的安全性问题成为当今最热门的话题之一，很多企业为了保障自身服务器或数据安全都采用了防火墙设置。随着科技的发展，防火墙也逐渐被大众所接受。

6.3.1　网络防火墙概述

1. 防火墙的概念

为了保护网络(特别是企业内部网——Intranet)资源的安全,人们创建了网络防火墙。就像建筑物防火墙或护城河能够保护建筑物及其内部资源安全或保护城市免受侵害一样,网络防火墙能够防止外部网上的各种危害侵入到内部网络。目前,防火墙已在 Internet 上得到了广泛的应用,并逐步在 Internet 之外得到应用。

网络防火墙是隔离在本地网络与外界网络之间所设立的执行访问控制策略的一道防御系统,它可防止发生不可预测的、外界对内部网资源的非法访问或潜在破坏性的侵入。应该说,在 Internet 上防火墙是一种非常有效的网络安全措施,通过它可以隔离风险区域(Internet 或有一定风险的网络)与安全区域(企业内部网,也可称为可信任网络)的连接,同时不会妨碍人们对风险区域的访问。

网络防火墙是目前实现网络安全策略的最有效的工具之一,也是控制外部用户访问内部网的第一道关口。防火墙的设置思想就是在内部、外部两个网络之间建立一个具有安全控制机制的安全控制点,通过允许、拒绝或重新定向经过防火墙的数据流,来实现对内部网服务和访问的安全审计和控制。防火墙虽然可以在一定程度上保护内部网的安全,但内部网还应有其他的安全保护措施,这是防火墙所不能代替的。客观地讲,防火墙并不是解决网络安全问题的万能药方,而只是网络安全政策和策略中的一个组成部分。

2. 防火墙的功能

防火墙的作用是防止不希望的、未授权的通信进出被保护的网络,使机构强化自己的网络安全政策。由于防火墙设定了网络边界和服务,因此更适合于相对独立的网络(如 Intranet)。事实上,在 Internet 上的 Web 网站中,超过三分之一的网站都是由某种形式的防火墙加以保护的。防火墙能够限制非法用户从一个被严格保护的设备上进入或离开,从而有效地阻止对内部网的非法入侵。但由于防火墙只能对跨越边界的信息进行检测、控制,而对网络内部人员的攻击不具备防范能力,因此单独依靠防火墙来保护内部网络的安全是不够的,还必须与入侵检测系统(IDS)、安全扫描、应急处理等其他安全措施综合使用才能达到目的。

一般来说,防火墙在配置上可防止来自"外部"未经授权的交互式登录,这大大有助于防止破坏者登录到网络用户的计算机上。一些设计更为精巧的防火墙既可以防止来自外部的信息流进入内部,又允许内部的用户可以自由地与外部通信。如果切断防火墙,就可以保护用户免受网络上任何类型的攻击。

防火墙的另一个非常重要的作用是可以提供一个单独的"阻塞点",在"阻塞点"上设置安全和审计检查。防火墙可提供一种重要的记录和审计功能:经常向管理员提供一些情况概要,提供有关通过防火墙的数据流的类型和数量,以及有多少次试图闯入防火墙的企图等信息。

6.3.2　防火墙技术

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术,越

来越多地被应用于专用网络与公用网络的互连环境中，尤其以接入 Internet 网络最普遍。防火墙可通过监测、控制跨越防火墙的数据流，尽可能地对外界屏蔽内部网络的信息、结构和运行状况，以此来实现内部网络的安全保护。

常用的防火墙技术有包过滤技术、代理服务技术、状态检测技术和自适应代理技术。通常也可将几种防火墙技术组合在一起使用，以弥补各自的缺陷，增加系统的安全性能。

1. 包过滤技术

包过滤(packet filtering)技术应用于网络层防火墙，该技术根据网络层和传输层的原则对传输的信息进行过滤。因此，利用包过滤技术在网络层实现的防火墙也称为包过滤防火墙。

包过滤技术在网络的出入口(如路由器)对通过的数据包进行检查和选择。选择的依据是系统内设置的过滤逻辑(包过滤规则)。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态或它们的组合，来确定是否允许该数据包通过。通过检查，只有满足条件的数据包才允许通过，否则被抛弃(过滤掉)。如果防火墙中设定某一 IP 地址的站点为不适宜访问的站点，则从该站点地址来的所有信息都会被防火墙过滤掉。这样可以有效地防止恶意用户利用不安全的服务对内部网进行攻击。包过滤防火墙要遵循的一条基本原则就是"最小特权原则"，即明确允许管理员希望通过的那些数据包，禁止其他的数据包。

在网络上传输的每个数据包都可分为数据和包头两部分。包过滤器就是根据包头信息来判断该包是否符合网络管理员设定的规则表中的规则，以确定是否允许数据包通过。包过滤规则一般是基于部分或全部报头信息的，如 IP 协议类型、IP 源地址、IP 选择域的内容、TCP 源端口号、TCP 目标端口号等。例如，包过滤防火墙可以对来自特定的 Internet 地址信息进行过滤，或者只允许来自特定地址的信息通过。如果将过滤器设置成只允许数据包通过 TCP 端口 80(标准的 HTTP 端口)，那么在其他端口，如端口 25(标准的 SMTP 端口)上的服务程序的数据包均不得通过。

包过滤防火墙既可以允许授权的服务程序和主机直接访问内部网络，也可以过滤指定的端口和内部用户的 Internet 地址信息。大多数包过滤防火墙的功能可以设置在内部网络与外部网络之间的路由器上，作为第一道安全防线。路由器是内部网络与 Internet 连接必不可少的设备，因此在原有网络上增加这样的防火墙软件几乎不需要任何额外的费用。

2. 代理服务技术

代理服务器防火墙工作在 OSI 模型的应用层，它掌握着应用系统中可用作安全决策的全部信息，因此，代理服务器防火墙又称应用层网关。这种防火墙通过一种代理(proxy)技术参与到一个 TCP 连接的全过程。

代理服务器是指代表客户处理在服务器连接请求的程序。当代理服务器得到一个客户的连接请求时，对客户的请求进行核实，并经过特定的安全化 proxy 应用程序处理连接请求，将处理后的请求传递到真正的 Internet 服务器上，然后接受服务器应答。代理服务器对真正服务器的应答做进一步处理后，将答复交给发出请求的终端客户。代理服务器通常运

行在两个网络之间，它对于客户来说像是一台真的服务器，而对于外部网的服务器来说，它又似一台客户机。代理服务器并非将用户的全部网络请求都提交给 Internet 上的真正服务器，而是先依据安全规则和用户的请求做出判断，是否代理执行该请求，有的请求可能被否决。当用户提供了正确的用户身份及认证信息后，代理服务器建立与外部 Internet 服务器的连接，为两个通信点充当中继。内部网络只接收代理服务器提出的要求，拒绝外部网络的直接请求。代理服务器的原理示意图如图 6.18 所示。

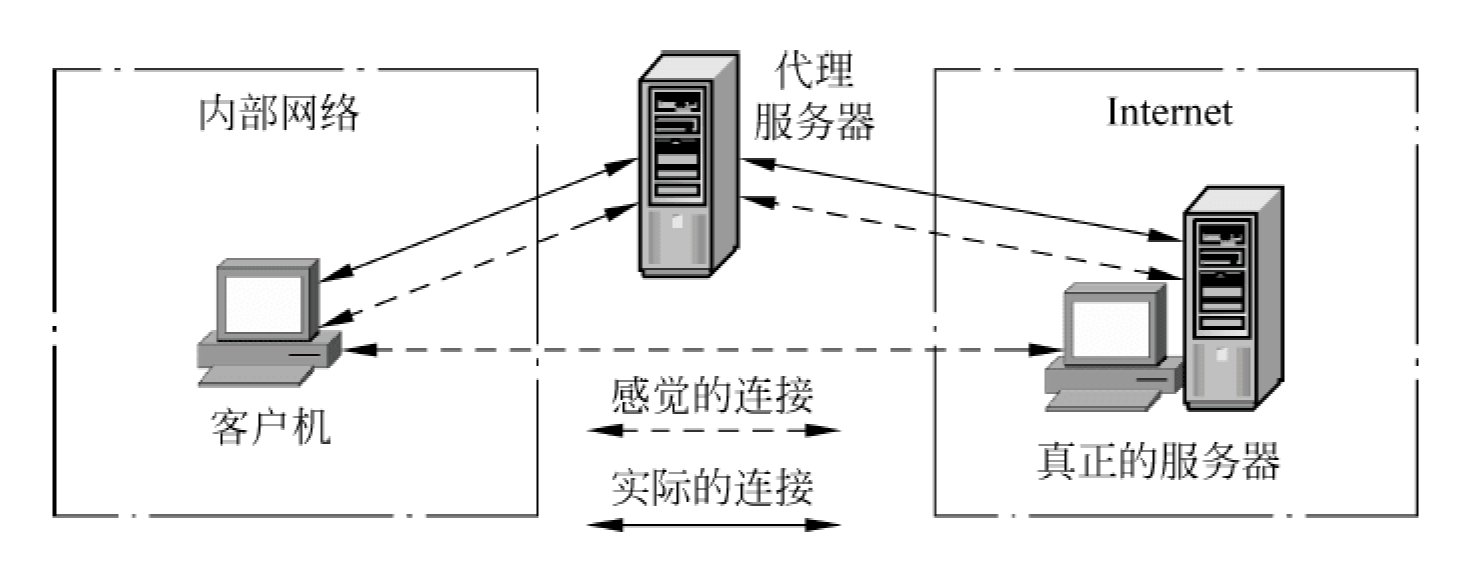


图 6.18　代理服务器的工作示意图

一个代理服务器本质上就是一个应用层网关，即一个为特定网络应用而连接两个网络的网关。代理服务器像一堵墙一样挡在内部用户和外界之间，分别与内部和外部系统连接，是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用。从外部只能看到该代理服务器而无法获知任何的内部资源(如用户的 IP 地址)。

代理服务可以实现用户认证、详细日志、审计跟踪和数据加密等功能，并实现对具体协议及应用的过滤，如阻塞 Java 或 Java Script。代理服务技术能完全控制网络信息的交换，控制会话过程，具有灵活性和安全性，但可能影响网络的性能，对用户不透明，且对每一种服务器都要设计一个代理模块，建立对应的网关层，实现起来比较复杂。

3. 状态检测技术

状态检测(stateful inspection)技术由 Check Point 率先提出，又称为动态包过滤技术。状态检测技术是新一代的防火墙技术。这种技术具有非常好的安全特性，它使用了一个在网关上执行网络安全策略的软件模块，称为检测引擎。检测引擎支持多种协议和应用程序，并可以很容易地实现应用和服务的扩充。与前两种防火墙不同，当用户访问请求到达网关的操作系统前，状态监视器要收集有关数据进行分析，结合网络配置和安全规定做出接纳或拒绝、身份认证、报警处理等动作。一旦某个访问违反了安全规定，该访问就会被拒绝，并报告有关状态，做日志记录。

状态检测技术监视和跟踪每一个有效连接的状态，并根据这些信息决定网络数据包是否能通过防火墙。它在协议栈底层截取数据包，然后分析这些数据包，并且将当前数据包和状态信息与前一时刻的数据包和状态信息进行比较，从而得到该数据包的控制信息，来达到保护网络安全的目的。

状态检测技术试图跟踪通过防火墙的网络连接和包，这样它就可以使用一组附加的标准，以确定是否允许和拒绝通信。状态检测防火墙是在使用了基本包过滤防火墙的通信上应用一些技术来做到这一点的。为了跟踪包的状态，状态检测防火墙不仅跟踪包中包含的

信息，还记录有用的信息以帮助识别包。

状态检测技术结合了包过滤技术和代理服务技术的特点。与包过滤技术一样的是它对用户透明，能够在 OSI 网络层上通过 IP 地址和端口号过滤进出的数据包；与代理服务技术一样的是可以在 OSI 应用层上检查数据包内容，查看这些内容是否能符合安全规则。

4. 自适应代理技术

自适应代理(adaptive proxy)技术本质上也属于代理服务技术，但它也结合了状态检测技术。自适应代理技术是最近在商业应用防火墙中实现的一种革命性的技术。它结合了代理服务防火墙的安全性和包过滤防火墙的高速度等优点，在保证安全性的基础上将代理服务器防火墙的性能提高 10 倍以上。

在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应代理的管理界面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务器从应用层代理请求，还是使用动态包过滤器从网络层转发包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

6.3.3 网络防火墙应用实例——Windows 防火墙的应用

Windows XP 的 Windows 防火墙是取代原来的 Internet 连接防火墙(ICF)的更新版本。ICF 是 Internet Connection Firewall 的简称，它建立在用户计算机与 Internet 之间，可以使用户请求的数据通过、阻碍没有请求的数据包，是一个基于包的防火墙。Windows 防火墙默认设置为开启状态，并且支持 IPv4 和 IPv6 两种网络协议，可以为用户的电脑提供更多的安全保护。在大多数情况下，系统会自动提醒用户进行安全设置，包括杀毒软件、防火墙以及系统补丁自动更新。当 Windows 防火墙打开后，如果设置得当可以从一定程度上加强系统的安全。

与 ICF 相比，Windows 防火墙的配置界面更加美观。Windows 防火墙还具有一些新的特性，如本地子网限制，应用到所有连接的通用配置选项，内建 IPv6 支持，新的组策略配置选项，可通过应用程序的文件名指定特定的通信(ICF 只能指定端口，而不能指定程序)等。

1. 打开 Windows 防火墙控制台

在 Windows XP 系统，执行“开始”→“设置”→“控制面板”命令，在控制面板中双击“Windows 防火墙”图标，打开“Windows 防火墙”控制台，如图 6.19 所示。

Windows 防火墙控制台窗口有常规、例外和高级三个选项卡。在“常规”选项卡中有“启用(推荐)”和“关闭(不推荐)”两个主选项，一个“不允许例外”子选项。“启用(推荐)”表示启用 Windows 防火墙；当选择“不允许例外”后 Windows 防火墙将拦截所有连接该计算机的网络请求，包括在例外标签中列表的应用程序和系统服务。此外，Windows 防火墙也将拦截文件和打印机共享，以及网络设备的侦测。使用“不允许例外”选项的 Windows 防火墙比较适用于连接在公共网络上的个人计算机，它拦截了绝大部分应用程序，但仍然可以浏览网页、发送和接收电子邮件、使用即时通信软件。



图 6.19　“Windows 防火墙”控制台

2. 添加例外程序或端口

当用户在本地运行一个应用程序并将其作为 Internet 服务器提供服务时，Windows 防火墙将会弹出一个新的安全警报对话框。通过对话框中的选项可以将此应用程序或服务添加到 Windows 防火墙的例外项中。Windows 防火墙的例外项配置将允许特定的进站连接。当然，也可以通过手工添加程序或添加端口到例外项中。

在图 6.19 中打开“例外”选项卡，如图 6.20 所示。在“程序和服务”栏中会显示通过 Windows 防火墙的程序和服务，选中的项表示可通过防火墙。在“例外”选项卡中有“添加程序”、“添加端口”、“编辑”和“删除”按钮。在此可根据具体的情况手工添加和删除例外项。在“添加程序”按钮下添加的是允许通过防火墙的程序。如果不清楚某个应用程序是通过哪个端口与外界通信，或者不知道它是基于 UDP 还是 TCP 的，可以通过“添加程序”来添加例外项。例如，要允许 Windows Messenger 通信，则单击“添加程序”按钮，选择应用程序“C:\Program Files\Messenger\Messenger\msmsgs.exe”，再单击“确定”按钮，即可将其加入列表。如果对端口号和 TCP/UDP 比较熟悉，则可单击“添加端口”按钮进行添加，即指定端口号添加。选中名称下的程序或者服务选项后，单击“添加端口”按钮可以更改应用程序的访问端口，输入名称后在端口号中输入允许的端口号，然后选中 TCP 或者 UDP 网络协议。选中名称下的程序或服务选项后，单击“编辑”按钮可以更改应用程序的访问范围。

对于每一个例外项，在“添加程序”或“添加端口”或“编辑”下均可以通过“更改范围”指定其作用域，如图 6.21 所示。对于家用和小型办公室应用网络，推荐设置作用域为可能的本地网络。当然，也可以自定义作用域中的 IP 范围，这样只有来自特定的 IP 地址范围的网络请求才能被接受。



图 6.20 使用防火墙的“例外”选项卡

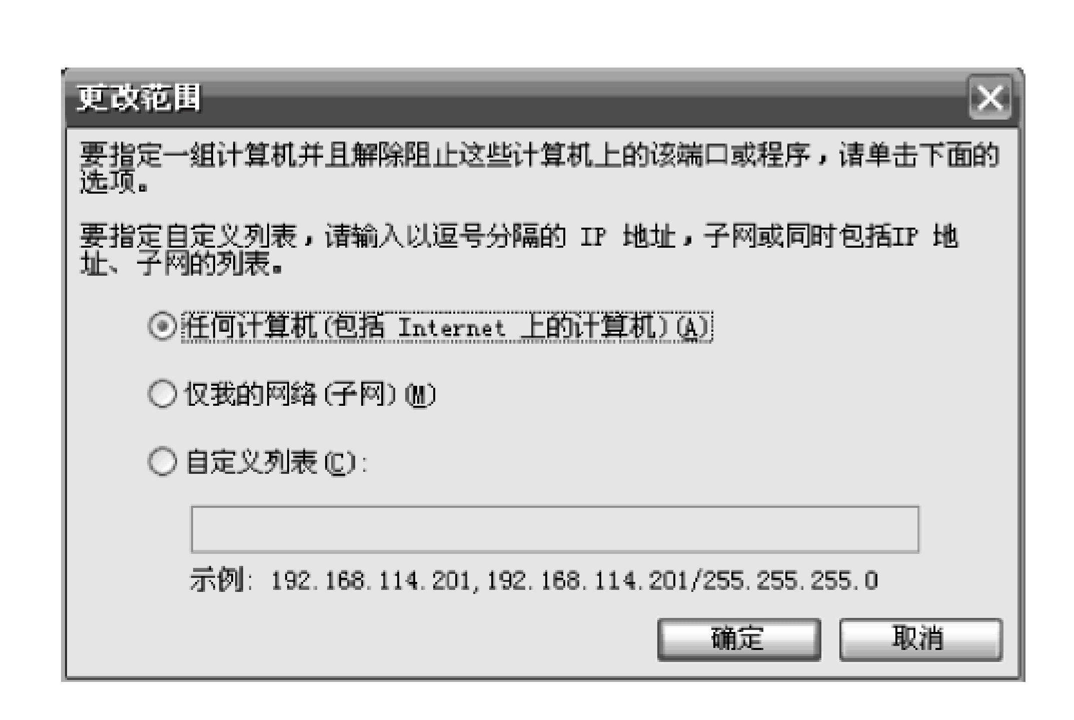


图 6.21 添加选项的更改范围

3. 网络连接设置

打开图 6.19 中的“高级”选项卡，弹出如图 6.22 所示的窗口。在“高级”选项卡中包含了“网络连接设置”、“安全日志记录”、“ICMP”和“默认设置”4 组选项，可以根据实际情况进行配置。

网络连接设置可选择 Windows 防火墙应用到哪些连接上，当然也可以对某个连接进行单独的配置，这样可以使防火墙应用更灵活。选择一个使用的连接，单击“设置”按钮进入“高级设置”对话框，如图 6.23 所示，有服务和 ICMP 两个选项卡。



图 6.22 “高级”选项卡



图 6.23 “高级设置”的“服务”选项卡

（1）服务设置

在“服务”选项卡中有 Windows XP 自带的一些服务，用户可选择自己想要的服务。如果觉得这些自带的服务不够或者不理想，可以单击“添加”按钮，手工添加自定义的服务，如图 6.24 所示。

（2）ICMP 设置

Internet 控制消息协议（ICMP）允许网络上的计算机共享错误和状态信息。在 ICMP 设置对话框中选定某一项时，界面下方会显示出相应的描述信息，可以根据需要进行配置。在默认状态下，所有的 ICMP 都没有打开。

打开 ICMP 选项卡，如图 6.25 所示。ICMP 是 Internet 控制信息协议，所有支持 TCP/IP 的网络都支持 ICMP。通过 ICMP 的反馈信息来确定网络的状态。在实际应用中，若要 ping 一个 IP 地址，就是 ICMP 把 ping 的结果返回给 ping 命令的发送者，从而让发送者知道网络的状态。



图 6.24　添加服务

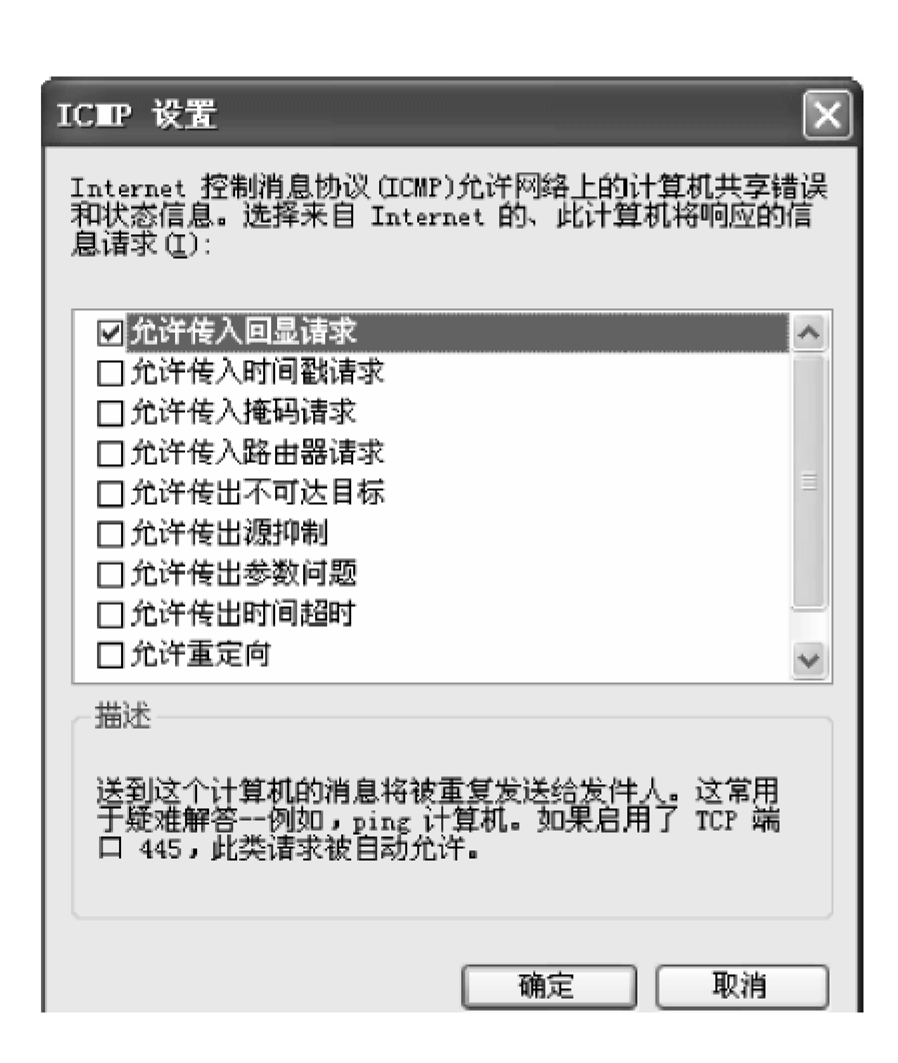


图 6.25　“高级设置”的 ICMP 选项卡

4. 安全日志设置

Windows 防火墙的安全记录功能可以提供一种方式来创建防火墙活动的日志文件，能够记录被许可的和被拒绝的通信。例如，默认情况下，防火墙不允许来自 Internet 的传入回显请求通过。如果没有启用 ICMP 的“允许传入的回显请求”项，那么传入请求将失败，并生成传入失败的日志项。在日志文件选项中，可以更改记录文件存放的位置，还可以手工指定日志文件的大小。

单击图 6.22 中“安全日志记录”的“设置”按钮，弹出如图 6.26 所示“日志设置”窗口。“记录选项”栏中的设置可以记录防火墙的跟踪记录，包括丢弃和成功的所有事项。Windows XP 默认的选项是不记录任何拦截或成功的事项，若要启用记录不成功的入站连接尝试，请选中“记录被丢弃的数据包”复选框，否则禁用。

通过“日志文件选项”可以更改记录文件存放的目录；生成安全日志时使用的格式是

W3C扩展日志文件格式，这与在常用日志分析工具中使用的格式类似。若要更改安全日志文件的路径和文件名，可单击图6.26中的"另存为"按钮，浏览选择要存放日志文件的位置。在"名称"文本框中，输入新的日志文件名，然后单击"确定"按钮，文件打开后可查看其内容。

通过"大小限制"可以修改记录文件的大小，避免过度占用空间。该项目的设置可以根据用户的需要进行。Windows XP记录文件的大小默认是4M(4096B)。



图6.26 设置防火墙日志

5. 默认设置

如果要将所有Windows防火墙设置恢复为默认状态，可在图6.22中的"默认设置"处单击"还原为默认值"按钮，即可将前面所有Windows防火墙设置还原为默认状态。

6. 组策略设置

Windows防火墙也可以通过组策略进行防火墙状态、允许的例外等设置。其操作过程如下：

第1步：选择"开始"→"运行"菜单，在"运行"对话框中输入gpedit.msc并按回车键，打开Windows XP组策略编辑器，如图6.27所示。进入组策略编辑器后，就可以用它配置Windows防火墙了。

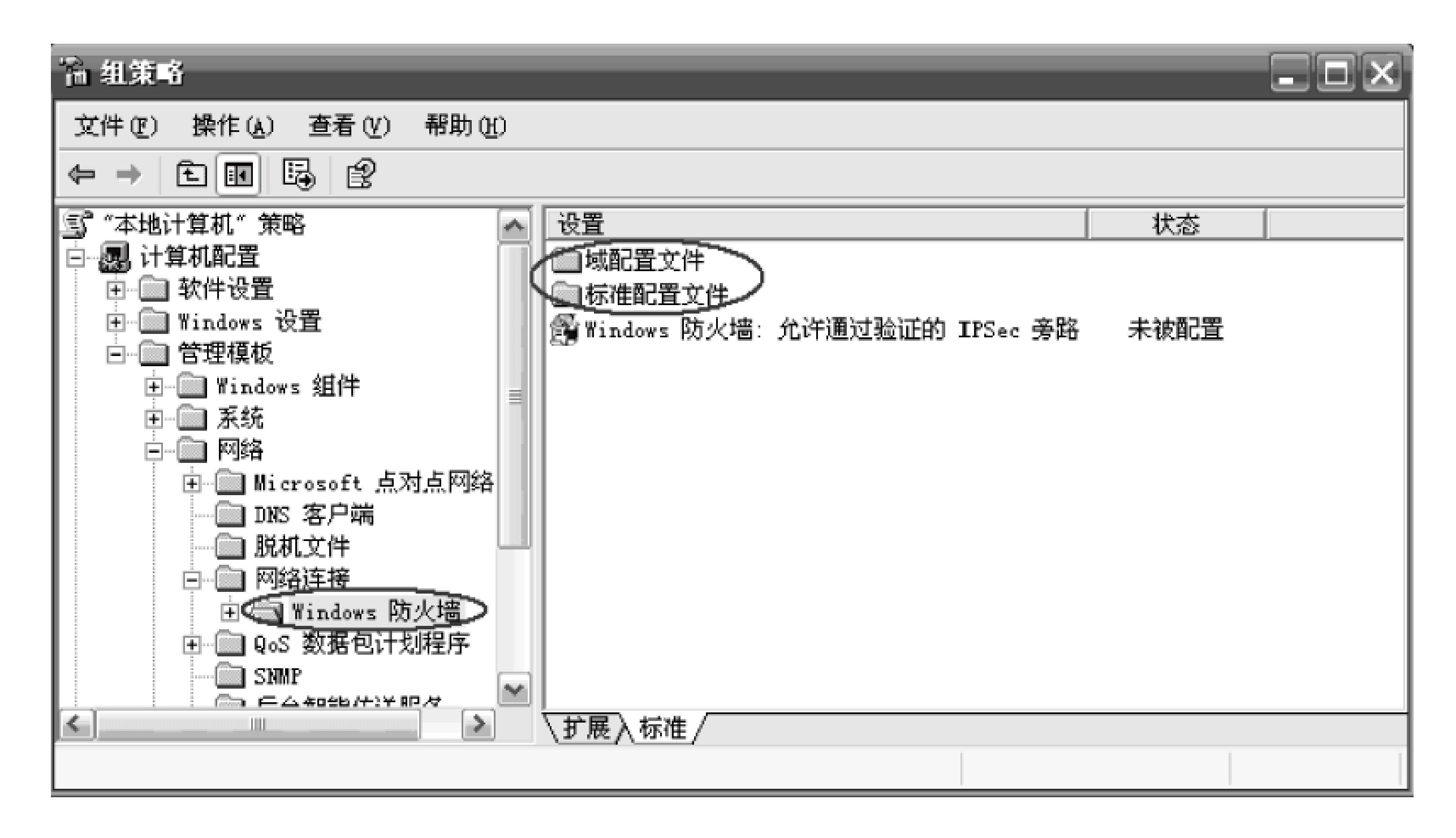


图6.27 Windows XP组策略编辑器

第2步：从左侧窗格中依次单击"计算机配置"→"管理模板"→"网络"→"网络连接"→"Windows防火墙"项。从图中Windows防火墙下可以看到两个分支设置，一个是域配置文件，一个是标准配置文件。当计算机连接到有域控制器的网络中(即有专门的管理服务器)时，是域配置文件起作用；否则，是标准配置文件起作用。即使没有配置标准配置文件，

默认的值也会生效。

7. 命令行配置

Windows 防火墙的配置和状态信息还可以通过命令行工具 Netsh.exe 进行。可在命令提示符窗口输入 netsh firewall 命令获取防火墙信息和修改防火墙设定。

netsh firewall 命令的参数及其含义如下：

- ?：显示命令列表。
- add：添加防火墙配置。
- delete：删除防火墙配置。
- dump：显示一个配置脚本。
- help：显示帮助列表。
- reset：将防火墙配置重置为默认值。
- set：设置防火墙配置。
- show：显示防火墙配置。

（1）使用 netsh firewall show allowedprogram 命令可查看 Windows 防火墙允许的应用程序。

（2）使用 netsh firewall show 命令可查看有关防火墙的帮助信息。

（3）使用 netsh firewall add allowedprogram 命令可添加防火墙允许的程序配置，如

```
add allowedprogram C:\MyApp\MyApp.exe MyApp ENABLE
```

表示允许 C:\MyApp\MyApp.exe 程序通过防火墙。

6.4　入侵检测系统与应用

入侵检测系统（Intrusion Detection System，IDS）是用来监视和检测入侵事件的系统。IDS 不仅能监测外来干涉的入侵者，同时也能监测内部的入侵行为，这就弥补了防火墙在这方面的不足。

6.4.1　入侵检测系统

1. IDS 的概念和功能

IDS 使网络安全管理员能及时地处理入侵警报，通过向管理员发出入侵或入侵企图来加强当前的访问控制系统，识别防火墙通常不能识别（如来自企业内部）的攻击，在发现入侵企图后提供必要的信息，提示网络管理员有效地监视、审计并处理系统的安全事件。由于入侵事件的危害越来越大，人们对 IDS 的关注也越来越多。对入侵攻击的检测与防范，保障计算机系统、网络系统及整个信息基础设施的安全等已经成为人们关注的重要课题。IDS 也已成为网络安全体系中的一个重要环节。

防火墙为网络安全提供了第一道防线，IDS 作为防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，提供对内部攻击、外部攻击和误操作的实时保护，

从而也极大地减少了网络各种可能攻击的危害。

与其他安全产品不同的是,IDS需要更多的智能。它必须能对得到的数据进行分析,并得出有用的结果。一个成功的IDS不但能大大简化管理员的工作,保证网络安全运行,使系统管理员时刻了解网络系统(包括程序、文件和硬件设备等)的任何变更,还能给网络安全策略的制定提供指导。入侵检测的规模应根据网络威胁、系统构造和安全需求的改变而改变。IDS在发现入侵后,会及时做出响应,包括切断网络连接、记录事件和报警等。

IDS通常具有以下功能。

① 监视用户和系统的运行状况,查找非法用户和合法用户的越权操作。

② 对系统的构造和弱点进行审计。

③ 识别分析著名攻击的行为特征并报警。

④ 对异常行为模式进行统计分析。

⑤ 评估重要系统和数据文件的完整性。

⑥ 对操作系统进行跟踪审计管理,并识别用户违反安全策略的行为。

⑦ 容错功能。即使系统发生崩溃,也不会丢失数据,或在系统重新启动时重建自己的信息库。

基于网络的入侵检测系统(NIDS)设置在比较重要的网段内,其数据源是网络上的数据包。NIDS往往将一台机器的网卡设为混杂模式,不停地监视本网段中的各种数据包,对每一个数据包进行特征分析和判断。如果数据包与系统内置的某些规则吻合,NIDS就会发出警报甚至直接切断网络连接。目前,大部分IDS产品是基于网络的。NIDS由遍及网络的传感器(sensor)组成,传感器是一台将以太网卡置于混杂模式的计算机,用于嗅探网络上的数据包。

NIDS的优点是能检测出来自网络的攻击和超过授权的非法访问,不影响机器的CPU、I/O与磁盘等资源的使用,系统发生故障时不影响正常业务的运行,系统安装方便,实时性好;NIDS的弱点是对加密通信无能为力,对高速网络无能为力,不能预测命令的执行后果。

2. 入侵检测技术

入侵检测技术是为保证计算机网络系统的安全而设计与配置的一种能够及时发现并报告系统异常现象的技术,是一种用于检测计算机网络中违反安全策略行为的技术。从具体的检测理论来看,IDS的检测分析技术主要有误用检测技术和异常检测技术两大类。

误用检测技术假定所有的入侵行为和手段都能够表达一种模式或特征。如果将以往发现的所有网络攻击的特征总结出来,并建立一个入侵信息库,则IDS可以将当前捕获到的网络行为特征与入侵信息库中的特征信息相比较,如果匹配,则当前行为就被认定是入侵行为。

异常检测技术是指根据用户的行为和系统资源的使用状况判断是否存在网络入侵。该技术首先假定网络攻击行为是不常见的或异常的,区别于所有的正常行为。如果能够为用户和系统的所有正常行为总结活动规律并建立行为模型,那么IDS可以将当前捕获到的网络行为与行为模型进行比较,若入侵行为偏离了正常行为轨迹,就可以被检测出来。

随着Internet的发展与广泛应用,无论从规模还是方法上,网络入侵的手段与技术也都有了进步与发展。入侵技术的发展主要反映出入侵的综合化与复杂化、主体对象的隐蔽化、

规模的扩大化和技术的分布化等特点。今后的入侵检测技术大致可向分布式入侵检测、智能化入侵检测、全面的安全防御方案、改进分析技术和高度可集成化等方向发展。

3. 入侵检测过程

从总体来说，IDS 进行入侵检测主要有信息收集和信息分析两个过程。

信息收集过程的收集内容包括系统、网络、数据及用户活动的状态和行为。应在网络系统中的若干不同关键点(不同网段和不同主机)收集信息。入侵检测很大程度上依赖于收集到的信息的可靠性和正确性。黑客对系统的修改可能使系统功能失常，但看起来与正常情况一样。这需要保证用来检测网络系统软件的完整性，特别是 IDS 软件本身应具有相当强的坚固性，防止因被篡改而收集到错误信息。

信息分析过程一般通过模式匹配、统计分析和完整性分析 3 种技术手段进行，主要是对收集到的系统、网络、数据及用户活动的状态和行为等信息进行分析。模式匹配就是将收集到的信息与已知的网络入侵和系统已有的模式数据库进行比较，从而发现违反安全策略的行为；统计分析为系统对象(如用户、文件、目录和设备等)创建一个统计描述，统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)，测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生；完整性分析利用强有力的加密机制来识别很微小的变化，关注某个文件或对象是否被更改。由此可见，模式匹配和统计分析方法用于实时入侵检测，而完整性分析则用于事后分析。

4. 入侵防护系统

防火墙旨在拒绝那些明显可疑的网络流量，但仍允许某些流量通过，因此它对很多入侵攻击无计可施。虽然 IDS 可以监视网络传输并发出警报，通过监视网络和系统资源，寻找违反安全策略的行为，但它并不能拦截攻击。因此 IDS 只能被动地检测攻击，而不能主动地把变幻莫测的威胁阻止在网络之外。目前，企业所面临的安全问题越来越复杂，如蠕虫、DDoS 攻击、垃圾邮件等极大地困扰着用户，给企业网络造成严重的破坏。因此，人们迫切需要找到一种主动防护入侵的解决方案，以确保企业网络在各种威胁和攻击的环境下正常运行。

入侵防护系统(Intrusion Prevention System，IPS)能提供主动性的防护，其设计旨在预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。IPS 是通过直接嵌入到网络流量中而实现这一功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，有问题的数据包和所有来自同一数据流的后续数据包都能够在 IPS 设备中被清除掉。

IPS 是一种主动的、积极的入侵防范和阻止系统。它部署在网络的进出口处，当它检测到攻击企图后，就会自动地将攻击包丢掉或采取措施将攻击源阻断。因此，从实用效果上看，与 IDS 相比，IPS 又有了新的发展，能够对网络起到较好的实时防护作用。

作为一种透明设施，IPS 是整个网络连接中的一部分。为了防止 IPS 成为网络中性能薄弱的环节，IPS 需要具有出色的冗余能力和故障切换机制，这样就可以确保网络在发生故障时依然能够正常运行。除了作为防御前沿，IPS 还是网络中的清洁工具，能够清除格式不

正确的数据包和非关键任务应用，使网络带宽得到保护。

基于网络的入侵防护系统(NIPS)通过检测流经的网络流量，提供对网络系统的安全保护。在技术上，NIPS 吸取了 NIDS 的所有成熟技术，包括特征匹配、协议分析和异常检测。特征匹配是最广泛的应用技术，具有准确率高、速度快等特点。IPS 不仅可进行检测，还能在攻击造成损坏之前阻断攻击，从而将入侵检测系统提升到一个新水平。

NIPS 工作在网络上，直接对数据包进行检测和阻断，与具体的主机/服务器操作系统平台无关。这种实时检测和阻断功能很有可能出现在未来的交换机上。随着处理器性能的提高，每一层次的交换机都有可能集成入侵防护功能。

6.4.2 入侵检测系统应用实例——Snort 软件工具的应用

Snort 是一个基于 libpcap 的、开放源代码的数据包嗅探器，并可以作为一个轻量级的网络入侵检测系统(NIDS)。轻量级是指在检测时尽可能少地影响网络的正常操作。Snort 可以运行在多种操作平台上，如 UNIX 系列(需要 libpcap 库支持)、Windows 系列(需要 winpcap 库支持)，与许多商业性产品相比，它对操作系统的依赖性较低。Snort 集成了多种报警机制以支持实时报警功能。目前，Snort 共有 30 多类近 2000 条检测规则，其中包括缓冲区溢出、端口扫描和 CGI 攻击等。

1. Snort 的安装

可以从网站 http://www.snort.org/或其他很多网站上下载 Snort 软件。如果用户安装了 libpcap，对 Snort 的安装非常简单。关于 libpcap 的安装说明，用户可阅读 blackfire 的一些文章。关于 Windows 下的 winpcap，用户可以查看 Sniffer For NT 上的安装说明。

安装好 Snort 后，用户可以使用 make clean 清除一些安装时产生的临时文件，而在 Windows 下更简单，只要解包出来就可以了。

2. Snort 命令介绍

命令行：

```
snort - [options] <filters>
```

选项[options]包括以下内容：

- -A <alert>：设置<alert>模式是 full、fast 或 none。full 模式记录标准的 alert 模式到 alert 文件中；fast 模式只写入时间戳、messages、IPs、ports 到文件中，none 模式关闭报警。
- -a：显示 ARP 包。
- -b：把 log 的信息包记录为 tcpdump 格式，所有信息包都被记录为二进制形式。Snort 在 100Mb/s 网络中使用-b 比较好。
- -c <cf>：使用配置文件<cf>，这个文件告诉系统什么样的信息要 log，或者报警，或者通过。
- -C：信息包数据使用 ASCII 码来显示，而不是 hexdump。
- -d：解码应用层。

- -D：把 Snort 以守护进程的方法来运行，默认情况下 alert 记录发送到/var/log/snort.alert 文件中。
- -e：显示并记录 ethernet 信息包头的数据。
- -F<bpf>：从<bpf>文件中读 BPF 过滤器(filters)。这里的 filters 是标准的 BPF 格式过滤器，用户可以在 tcpdump 里看到，可以查看 tcpdump 主页了解过滤器的使用。
- -h <hn>：设置网络地址。
- -I <if>：使用网络接口参数<if>。
- -l <ld>：log 信息包记录到<ld>目录中。
- -n <num>：指定在处理<num>个数据包后退出。
- -N：关闭 log 记录，但 alert 功能仍正常。
- -o：改变所采用的记录文件。如正常情况下采用 alert→pass→log 顺序，而采用此选项后的顺序为 pass→alert→log。pass 是那些允许通过的规则而不记录和报警，alert 是不允许通过的规则，log 指 log 记录。
- -p：关闭混杂模式嗅探方式，一般用于安全的调试网络。
- -r <tf>：读取由 tcpdump 方式产生的文件<tf>。这个方法可用来处理类似 Shadow 的文件，因为这样的文件不能用一般的 edit 来编辑查看。
- -s：log 报警记录到 syslog 中。在 Linux 平台上，这些警告信息会出现在/var/log/secure 中，在其他平台上出现在/var/log/message 中。
- -S <n=v>：设置变量值。可以在命令行定义 Snort rules 文件中的变量，如用户要在 Snort rules 文件中定义变量 HOME_NET，用户可以在命令行中给它预定义值。
- -v：使用 verbose 模式，把信息包打印在 console 中。使用这个选项会使速度变慢，在记录多的时候会出现丢包现象。
- -V：显示 snort 版本并退出。

3. Snort 的应用

Snort 有 3 种工作模式：嗅探器、数据包记录器和 NIDS 系统。嗅探器模式仅仅是从网络上读取数据包并作为连续不断的数据流显示在终端上；数据包记录器模式把数据包记录到硬盘上；NIDS 模式是最复杂的，而且是可配置的。

(1) 嗅探器模式

嗅探器模式就是 Snort 从网络上读出数据包然后显示在客户机。用户要想把 TCP/IP 信息包头显示在屏幕上，可以使用命令：

```
./snort -v
```

如果要想看到应用层的数据(解码应用层)，可以使用：

```
./snort -vd
```

这条命令使 Snort 在输出包头信息的同时显示包的数据信息。如果要查看到更详细的关于 ethernet 头的信息，可使用下面的命令：

```
./snort -vde
```

这些选项还可分开写或任意结合在一块。例如下面的命令与上面的命令等价：

```
./snort -d -v -e
```

(2) 数据包记录器模式

在嗅探器模式下，用户只在屏幕上可看到上述命令。如果要把所有的数据包记录到硬盘上，需要指定一个日志目录，Snort 就会自动记录数据包。用户可以先建立一个 log 目录，再使用下面的命令：

```
./snort -dev -l ./log -h 192.168.1.0/24
```

该命令把 ethernet 头信息和应用层数据记录到./log 目录中，记录内容是关于 C 类网络 192.168.1.0 的信息。如果用户想利用一些规则文件(记录特定数据的规则文件)，则使用命令：

```
./snort -dev -l ./log -h 192.168.1.0/24 -c snort-lib
```

此处 snort-lib 是用户规则文件的文件名，按照 snort-lib 文件中设置的规则决定是否记录某个信息包。而命令行“./snort -d -h 192.168.1.0/24 -l ./log -c snort-lib”可以不记录 ethernet 头信息。

命令行“./snort -d -h 192.168.1.0/24 -l ./log -c snort-lib -s”可把日志记录在用户规则文件所定义的 log 文件中，而不是默认的 alert.ids 中。

命令行“./snort -d -h 192.168.1.0/24 -l ./log -c snort-lib -o”是读规则文件的顺序。如果需要先读允许的规则文件，再读 alert 规则文件，然后来 log 记录，那就按照上面的命令操作。

如果用户的网络请求相当多，用户可以使用命令行：

```
./snort -b -A fast -c snort-lib
```

用户可以使用如下命令查看 log：

```
./snort -d -c snort-lib -l ./log -h 192.168.1.0/24 -r snort.log
```

如果用户的网络速度很快，或者想使日志更加紧凑以便以后的分析，则应使用二进制的日志文件格式。二进制日志文件格式就是 tcpdump 程序使用的格式。使用下面的命令可把所有的包记录到一个二进制文件中：

```
./snort -l ./log -b
```

(3) NIDS 模式

Snort 最重要的用途是作为 NIDS，使用下面命令行可启动该模式：

```
./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf
```

snort.conf 是规则集文件。Snort 会对每个包和规则集进行匹配，发现这样的包就采取相应的行动。如果不指定输出目录，Snort 就输出到/var/log/snort 目录。

如果想长期使用 Snort 作为自己的 NIDS，最好不要使用-v 选项。因为使用该选项会使 Snort 向屏幕上输出一些信息，将大大降低 Snort 的处理速度，从而在向显示器输出的过程中丢弃一些包。此外，在绝大多数情况下，也没有必要记录 ethernet 包头信息，所以-e 选项也可以不用。

命令行“./snort -d -h 192.168.1.0/24 -l ./log -c snort.conf”是使用 snort 作为 NIDS 最基本的形式，将符合规则的日志包以 ASCII 形式保存在有层次的目录结构中。

在 NIDS 模式下，有很多方式来配置 Snort 的输出。在默认情况下，Snort 以 ASCII 格式记录日志，使用 full 报警机制。如果使用 full 报警机制，Snort 会在包头之后打印报警消息。如果不需要日志包，可以使用-N 选项。

Snort 有 6 种报警机制：full、fast、unsock、none、syslog 和 smb(winpopup)，其中前 4 种可以在命令行状态下使用-A 选项设置。

- -A fast：报警信息，包括一个时间戳(timestamp)、报警消息、源/目的 IP 地址和端口。
- -A full：默认报警模式。
- -A unsock：把报警发送到一个 UNIX 套接字，需要有一个程序进行监听，这样可以实现实时报警。
- -A none：关闭报警机制。

使用-s 选项可以使 Snort 把报警消息发送到 syslog，默认的设备是 LOG_AUTHPRIV 和 LOG_ALERT。可以修改 snort.conf 文件改变其配置。

Snort 还可以使用 SMB 报警机制，通过 SAMBA 把报警消息发送到 Windows 主机。为了使用这个报警机制，在运行./configure 脚本时，必须使用 enable-smbalerts 选项。

下面是一些输出配置的实例：

使用默认的日志方式并把报警发给 syslog：

```
./snort -c snort.conf -l ./log -s -h 192.168.1.0/24
```

使用二进制日志格式和 SMB 报警机制：

```
./snort -c snort.conf -b -M WORKSTATIONS
```

使用-r 功能开关，也能使 Snort 读出包的数据。Snort 在所有运行模式下都能够处理 tcpdump 格式的文件。如果想在嗅探器模式下把一个 tcpdump 格式的二进制文件包打印到屏幕上，可以输入以下命令行：

```
./snort -dv -r packet.log
```

在日志包和入侵检测模式下，通过 BPF(BSD packet filter)接口，可使用许多方式维护日志文件中的数据。例如，若只想从日志文件中提取 ICMP 包，只需要输入如下命令即可：

```
./snort -dvr packet.log icmp
```

6.5 网络扫描与网络监听

6.5.1 网络扫描

影响网络系统安全的因素很多,但不外乎来自系统内部的漏洞(缺陷或脆弱性)和来自网络系统外部的威胁。

网络扫描是保证网络系统安全必不可少的手段,它不仅可以实现复杂繁琐的信息系统安全管理,而且可从目标信息系统和网络资源中采集信息,帮助用户及时找出网络中存在的漏洞,分析来自网络外部和内部的入侵信号和网络系统中的漏洞,有时还能实时地对攻击做出反应。

1. 网络系统漏洞

在计算机网络安全领域,网络系统漏洞是指网络系统硬件、软件或策略上存在的缺陷或脆弱性。计算机网络本身存在着一些漏洞,非授权用户利用这些漏洞可对网络系统进行非法访问。这种非法访问可能使系统内数据的完整性受到威胁,也可能使信息遭到破坏而不能继续使用,更为严重的是有价值的信息被窃取而不留任何痕迹。

计算机网络系统的硬件和软件缺陷可影响系统的正常运行,严重时系统会停止工作。

网络系统硬件的缺陷主要有硬件故障、网络线路威胁、电磁辐射和存储介质脆弱等方面。

网络系统的软件漏洞是指在计算机程序、系统或协议中存在的安全漏洞,它已成为被攻击者用来非法侵入他人系统的主要渠道。软件方面的漏洞可分为应用软件漏洞、操作系统漏洞、数据库系统漏洞、通信协议漏洞和网络软件及网络服务漏洞。

一般来说,软件漏洞一旦被检测出来,相关的软件厂商都会在最短时间内发布相应的补丁程序。但是问题在于当黑客发现漏洞存在后,就会尽快设计出一种可利用这些漏洞的新型恶意代码对系统进行攻击。针对各种软件漏洞,最好的应对策略就是下载相应的补丁程序。

2. 网络扫描

网络扫描通常采用两种策略:一种是被动式策略;另一种是主动式策略。被动式策略是基于主机的,对系统中不合适的设置、脆弱的口令以及其他与安全规则抵触的对象进行检查;主动式策略是基于网络的,通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应,从而发现其中的漏洞。

(1) 扫描器

对付破坏系统企图的实用方法,就是建立比较容易实现的安全系统,同时按照一定的安全策略建立相应的安全辅助系统。网络扫描程序(扫描器)就是这样一类实用的安全系统。

在 Internet 安全领域,扫描器是最出名的破解工具。扫描器实际上是一种自动检测远程或本地主机安全性弱点的程序。通过与目标主机 TCP/IP 端口建立连接,并请求某些服务(如 Telnet、FTP),记录目标主机的应答,搜集目标主机相关的信息,以此获得关于目标机

的信息，理解和分析这些信息，就可能发现破坏目标主机安全性的关键问题。扫描器的重要性在于把极为复杂的安全检测，通过程序来自动完成，这不仅减轻了管理者的工作，而且缩短了检测时间。一个好的扫描器能对它得到的数据进行分析，帮助查找目标主机的漏洞。但它不会提供进入一个系统的详细步骤。

扫描器的主要功能是测试系统上有没有安全漏洞，进而从扫描出来的安全漏洞报告里告诉使用者，系统安全漏洞有多少，如何去修补，到哪里下载 Patches（补丁程序）等。

根据工作模式的不同，扫描器一般可分成网络型扫描器和主机型扫描器两大类，其中前者基于网络，通过请求/应答方式远程检测目标网络和主机系统的安全漏洞；后者基于主机，通过在主机系统本地运行代理程序来检测系统漏洞，如操作系统漏洞扫描器和数据库系统漏洞扫描器。

主机型扫描器具有重要资料的锁定、密码检测、系统日志文件和文字文件分析、加密和分析报表等功能。

（2）端口扫描

网络上计算机之间的通信都是通过端口进行的，不同的通信内容被分派在不同的端口上。端口扫描的目的是探测主机开放了哪些端口。实现的方法是对目标主机的每个端口发送信息，用扫描器针对目标主机查询，最终就会查出哪些主机开放了哪些端口。某些特定的端口是一些服务或程序默认的。一些安全服务器可能会更改默认端口，这样就比较安全了，因为改变端口就可以起到迷惑攻击者的目的。

一个端口就是一个潜在的入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息，从而发现系统的安全漏洞。支持 TCP/IP 协议的主机和设备，都是以开放端口来提供服务的。端口是系统对外的窗口，漏洞也往往通过端口暴露出来。因此，网络扫描器为了提高扫描效率，首先需要判断系统的哪些端口是开放的，然后对开放的端口执行某些扫描脚本，以进一步寻找安全漏洞。

常见的 TCP 端口有 21H（FTP）、23H（Telnet）、25H（SMTP）、70H（Gopher）、79H（Finger）、80H（HTTP）、110H（POP3）、119H（News Server）、139H（NetBIOS）等；常见的 UDP 端口有 53H（DNS）、69H（TFTP）、88H（Kerberos）、110H（POP3）、119H（News Server）、139H（NetBIOS）等。

6.5.2　网络监听

网络监听是管理员为了进行网络安全管理，利用相应的工具软件监视网络的状态和数据流动情况，以便及时发现网络中的异常情况和不安全因素。网络管理员使用网络监听工具软件可以监视网络的状态、数据流动以及网络上传输的信息。

1. 网络监听的概念

网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网络的 Modem 之间等。但监听效果最好的地方是在网关、路由器、防火墙一类的设备处，使用最方便的是在一个以太网中的任何一台上网的主机上进行监听。对于一台连网的计算机，最方便的是在以太网中进行监听。只需安装一个监听软件，然后就可以坐在机器旁浏览监听到的信息了。

在一般的网络环境下用户的信息(包括口令)都是以明文方式传输的,通过网络监听而获得用户信息并不是一件很难的事情,只要掌握初步的TCP/IP协议知识就可以轻松地做到了。网络监听也是一把“双刃剑”,既可以为网络管理员所用监视网络的状态和数据流动情况,也可被黑客利用起破坏作用。因此网络监听也是黑客们常用的手段之一。当信息以明文形式在网络上传输时,黑客便可以将网络接口设置为监听模式,使用网络监听手段截获网上数据,便可以源源不断地将网上传输的信息截获。当黑客成功地登录一台网络主机并取得该主机的超级用户权限后,往往要扩大战果,尝试登录或夺取对网络中其他主机的控制权。

对于网络攻击者来说,攻破网关、路由器或防火墙的难度很大。因为在这些地方可以由安全管理员安装一些设备,对网络进行监控,或使用一些专门的设备,运行专门的监听软件。但攻击者潜入一台不引人注意的计算机中,悄悄地运行一个监听程序是很容易的。监听非常消耗CPU资源,在一个担负繁忙任务的计算机中进行监听,可能会立即被管理员发现,因为计算机的响应速度会变得很慢。

2. 网络监听的检测

网络监听的前提条件是在同一网段的主机上进行。这里同一网段是指物理上的连接。因为不同网段的数据包在网关就会被滤掉,不能传输到另外的网段,否则一个Internet上的一台主机便可以监视整个Internet了。

网络监听是很难被发现的。运行网络监听程序的主机只是被动地接收在局域网上传输的信息,并没有主动的行动。既不会与其他主机交换信息,也不能修改在网上传输的信息包。这些都决定了对网络监听的检测是非常困难的。

一个理论上可行的检测监听的办法是搜索所有主机上运行的进程。但这几乎是不可能的,因为很难同时检查所有主机上的进程。但至少管理员可以确定是否有一个进程被从管理员机器上启动。

一般来讲,人们真正关心的是那些秘密数据(如用户名和口令)的安全传输。如果这些信息以明文形式传输,就很容易被截获而且被阅读,因此对信息进行加密是一个很好的办法。如果利用安全外壳SSH(secure shell)协议进行加密是很容易实现的,而且效率很高。SSH是一种在像Telnet那样的应用环境中提供保密通信的协议,它可实现密钥交换、主机认证和客户端认证,可完全排除在不安全的信道上通信被监听的可能性。它像许多协议一样,是建立在客户/服务器模型之上的。

3. 网络监听的防范

(1) 从逻辑或物理上对网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段,其实也是保证网络安全的一项措施。其目的是将非法用户与敏感的网络资源相互隔离,从而防止可能的非法监听。

(2) 使用交换式集线器

对局域网的中心交换机进行网络分段后,局域网监听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机。分支集线器通常是共享式的,当用户与主机进行数据通信时,两台计算机之间的数据包可能被同一台集线器上的其他用

户所监听。因此，要以交换式集线器代替共享式集线器，使数据包仅在两个节点间传送，从而可防止非法监听。

（3）使用加密技术

数据经过加密后，虽然通过监听仍然可以得到传送的信息，但这些信息是无法理解的密文。加密会影响数据传输速度，系统管理员和用户需要根据网络速度和安全性要求进行考虑。

（4）划分 VLAN

运用 VLAN（虚拟局域网）技术，将以太网的广播式通信变为点到点通信，这样可以防止大部分基于网络监听的入侵。

6.5.3　网络扫描应用实例——X-Scan 扫描软件的应用

X-Scan v3.3 是一款完全免费且非常优秀的综合扫描器软件，主要由国内著名的民间黑客组织“安全焦点”（http://www.xfocus.net）开发。该软件采用多线程方式对指定 IP 地址段或单机进行安全漏洞检测，支持插件功能。它提供了图形界面和命令行两种操作方式，其系统要求是 Windows NT/2000/XP/2003。可以利用该软件对系统存在的一些漏洞进行扫描。扫描内容包括远程服务类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等多个大类。对于多数已知漏洞，通过扫描可给出相应的漏洞描述、解决方案及详细描述链接。

X-Scan v3.3 的主界面如图 6.28 所示，其应用过程如下。



图 6.28　X-Scan v3.3 软件主界面

1. 设置扫描范围和扫描模块

选择图 6.28 中菜单栏“设置”下的“扫描参数”项，在扫描参数中设置检测范围。本例设定的“扫描范围”为 202.120.30.1—202.120.30.161，如图 6.29 所示。

扫描模块的设置如图 6.30 所示。设置完毕后，即可进行漏洞扫描。

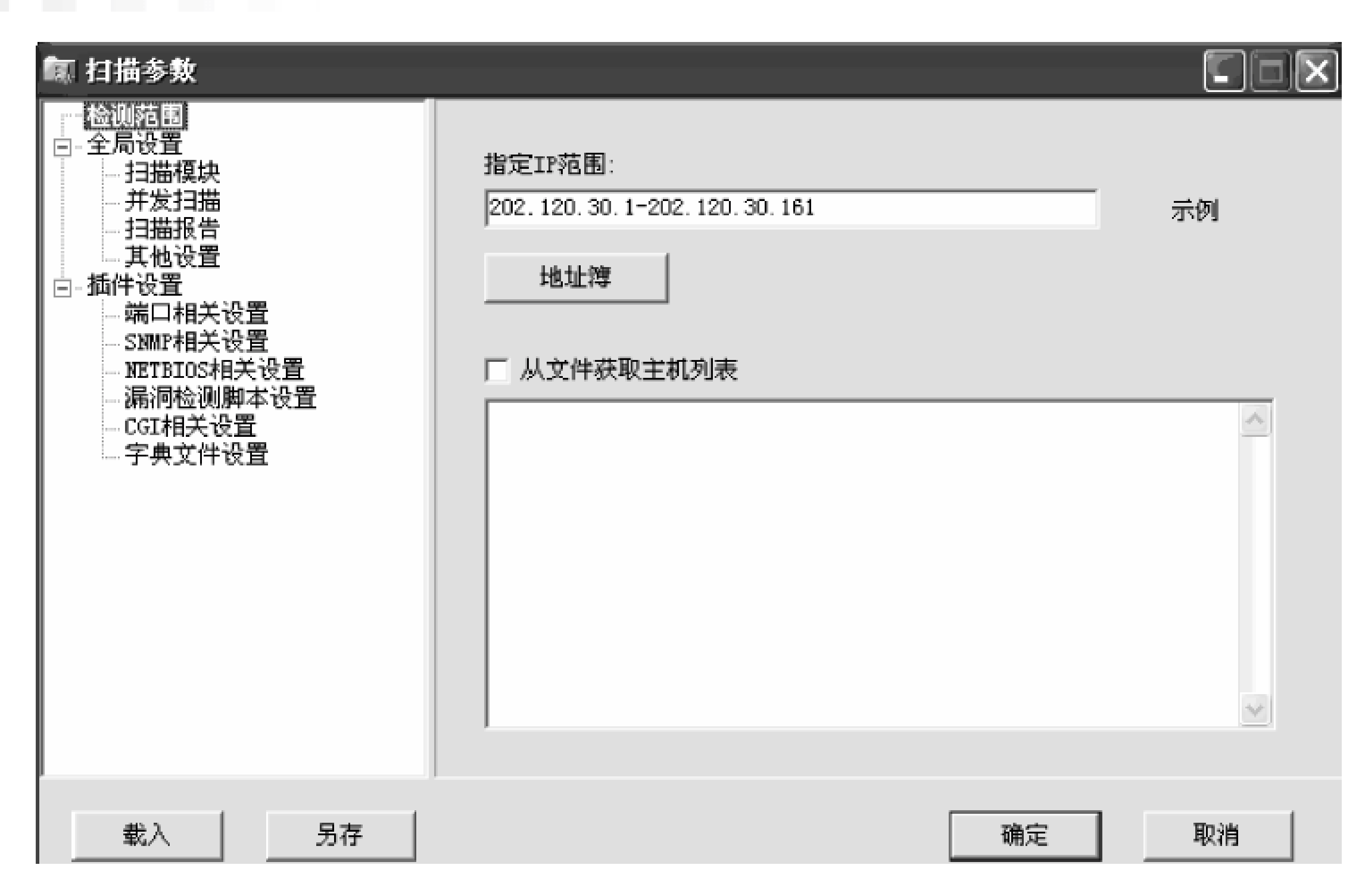


图 6.29 扫描范围设置窗口



图 6.30 扫描模块设置

2. 进行漏洞扫描

打开图 6.28 中的“文件”菜单，选择“开始扫描”选项，系统即开始扫描。图 6.31 所示为扫描检测过程，从中可见本次扫描检测出两个存活主机 202.120.30.160 和 202.120.30.5。

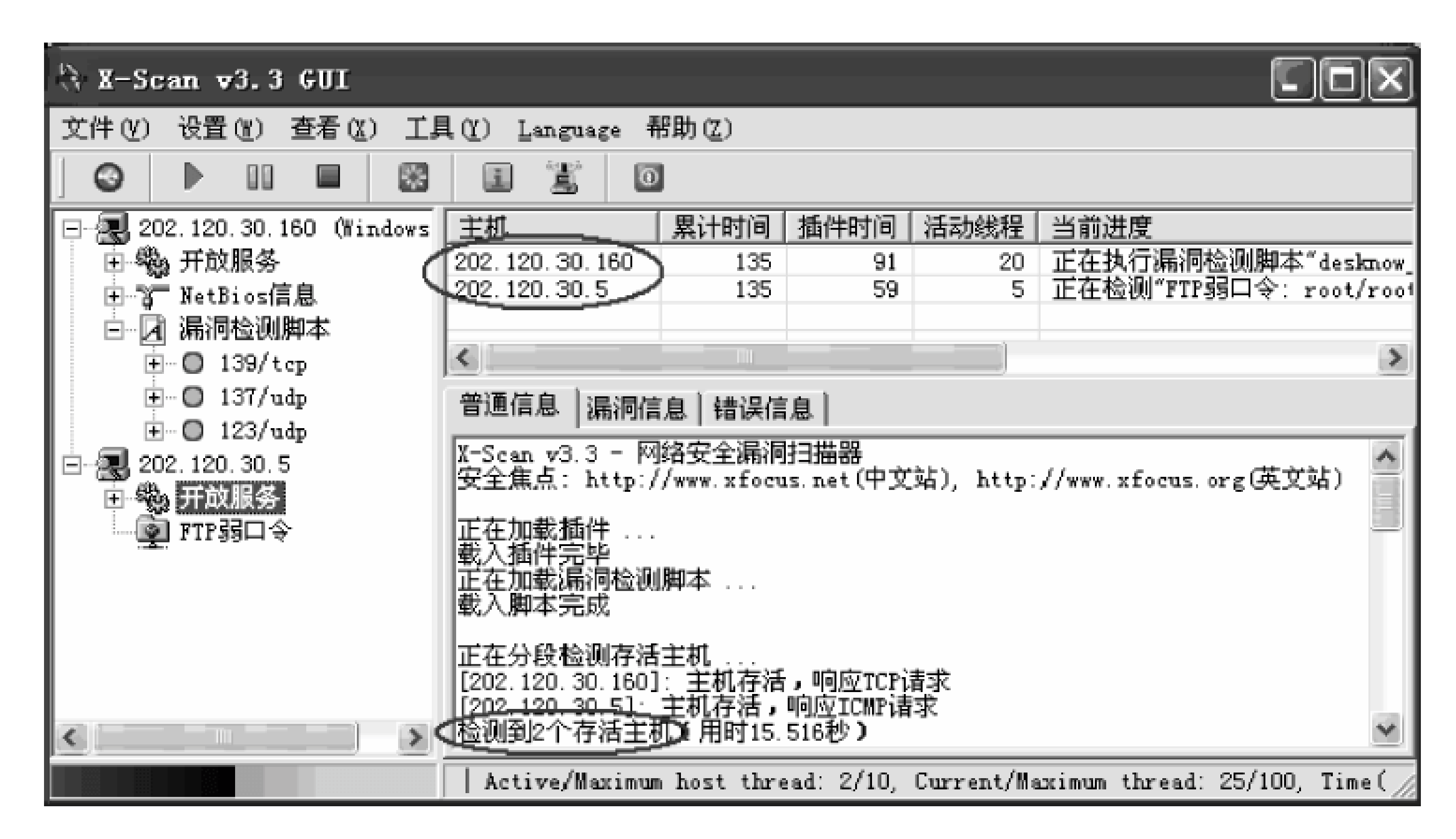


图 6.31 扫描检测过程

图 6.32 为扫描检测报告，报告显示本次扫描用时近 13 分钟。检测结果是两个存活主机均发现安全提示。图 6.33 和图 6.34 分别为 202.120.30.5 和 202.120.30.160 的主机分析(部分)报告。图 6.35 为扫描报告的另一种显示。

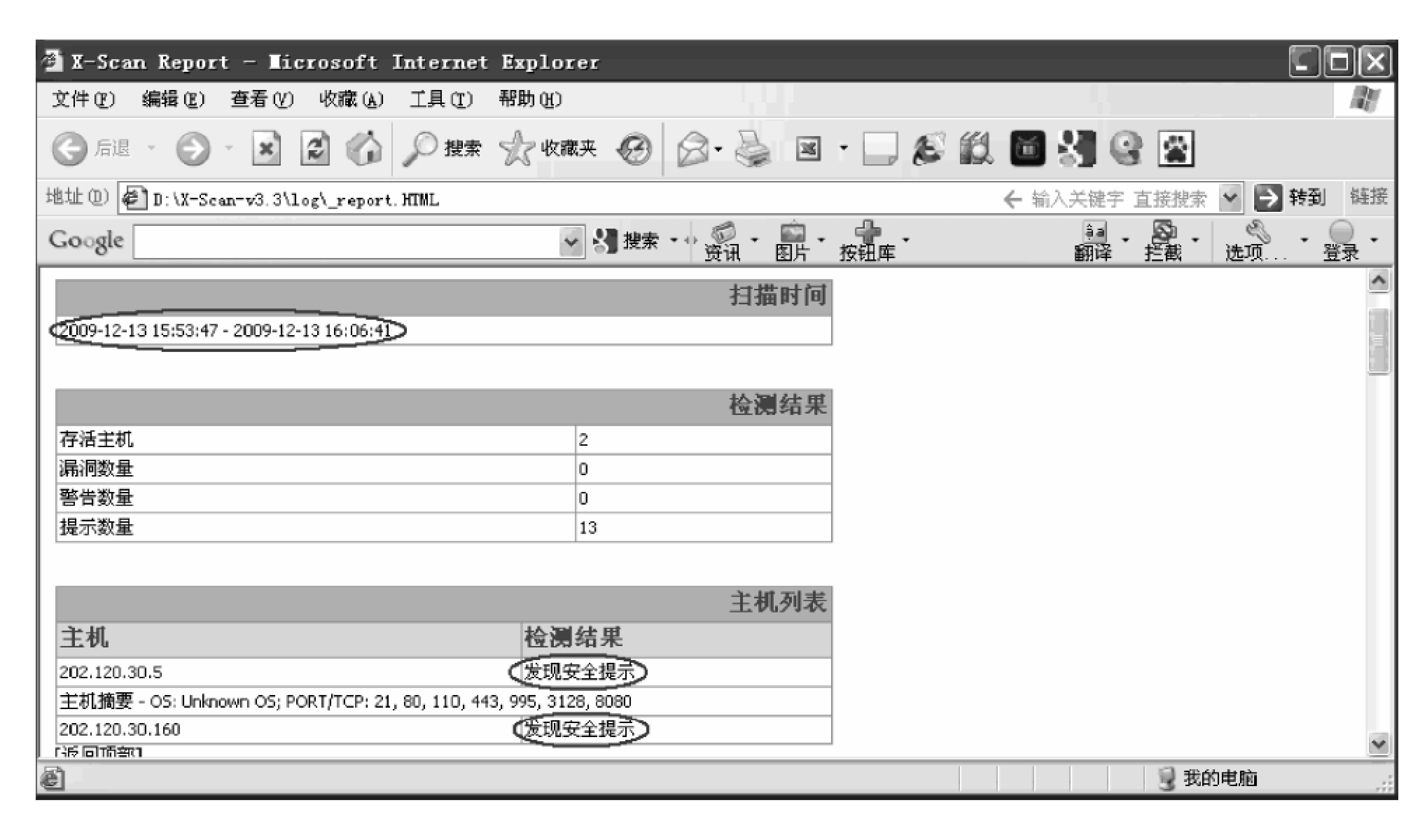


图 6.32 扫描检测报告(1)



图 6.33 扫描检测报告(2)

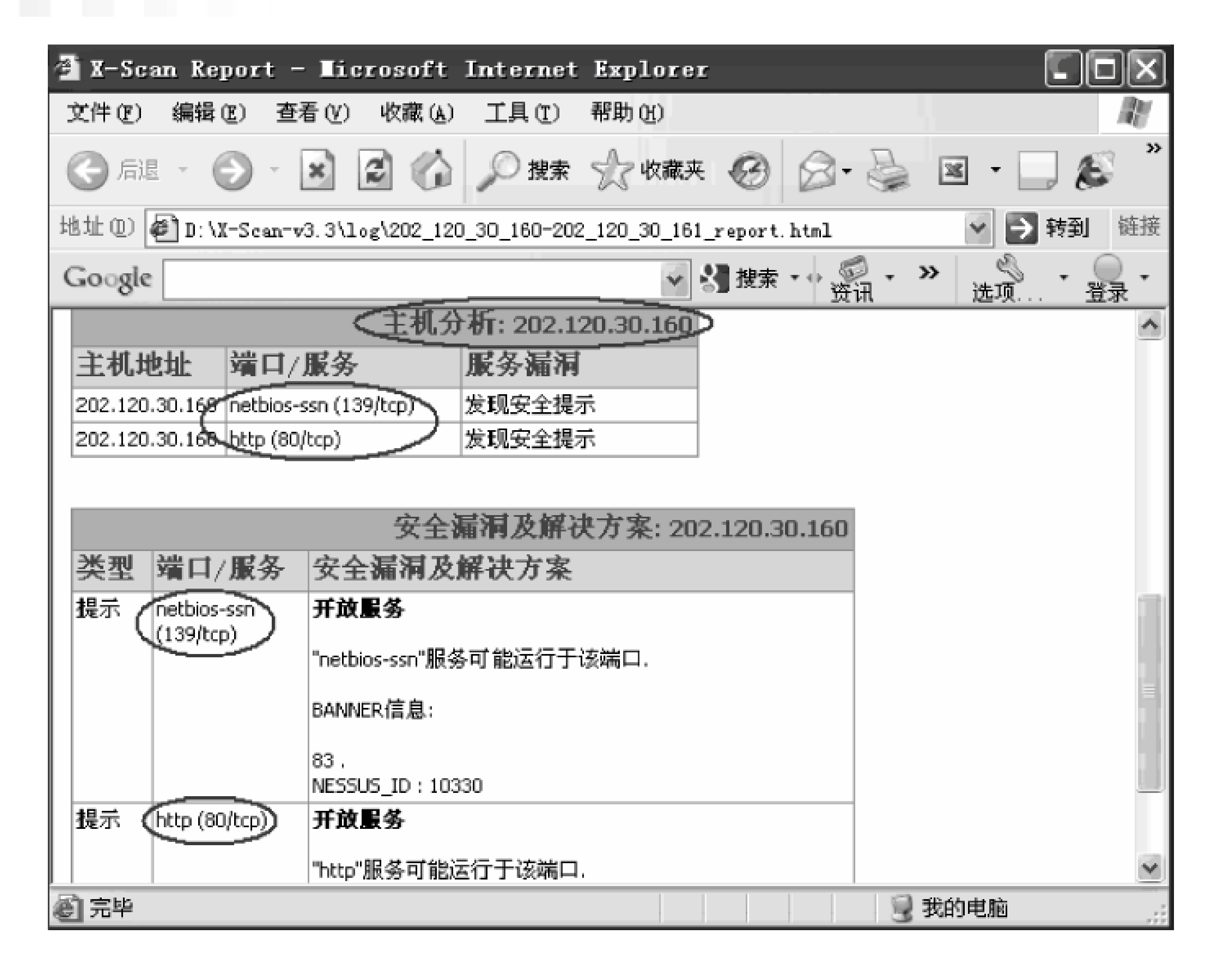


图 6.34 扫描检测报告(3)

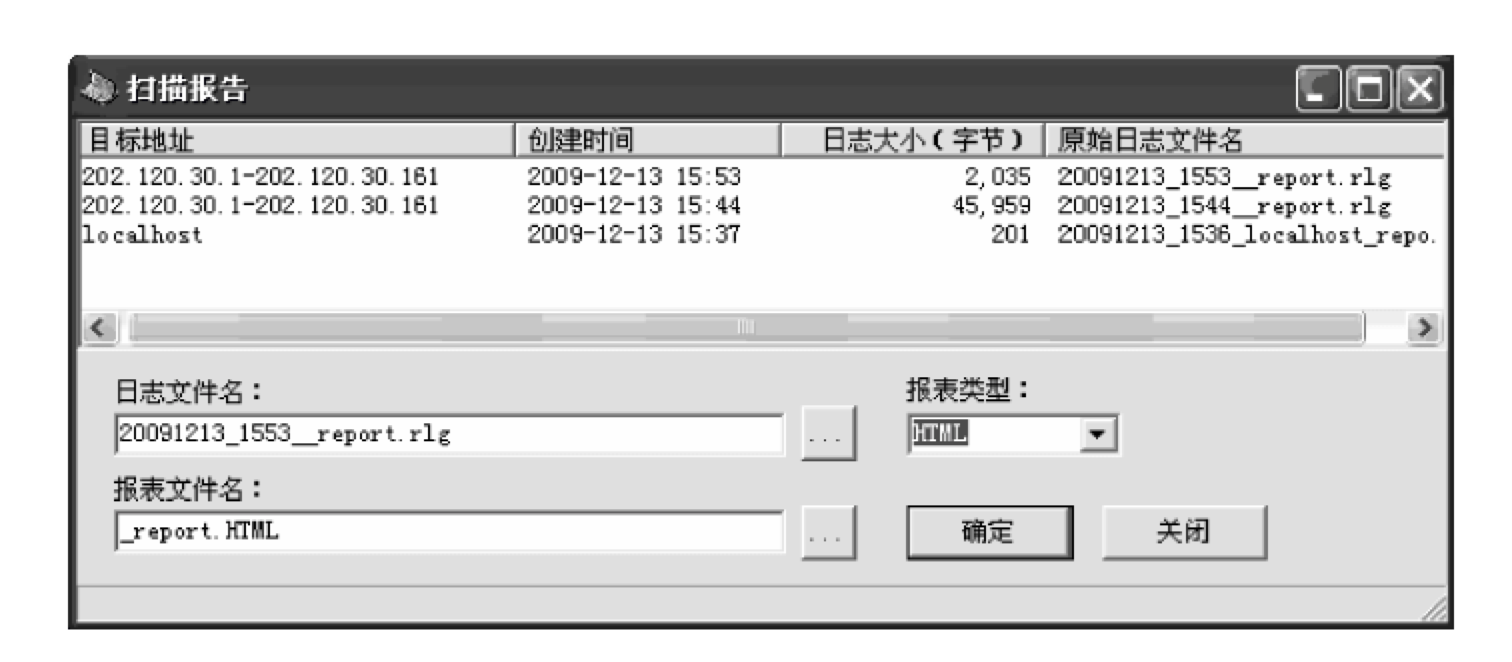


图 6.35 扫描检测报告(4)

3. 查询主机的域名和地址

打开图 6.28 中的"工具"菜单,选择"物理地址查询"选项,弹出如图 6.36 所示的窗口。在该窗口中,可查询到已知域名的 IP 地址,如图 6.36 和图 6.37 所示,也可查询到已知 IP 地址所对应的域名,如图 6.38 和图 6.39 所示。

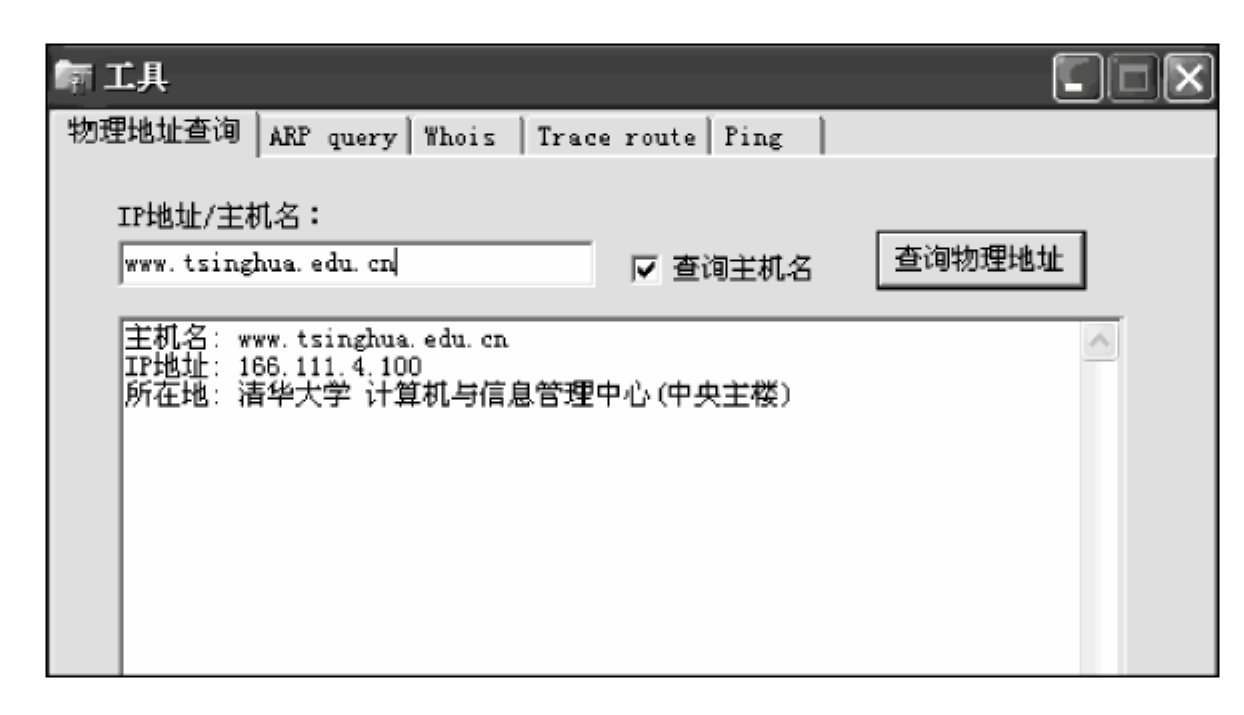


图 6.36 查询已知域名的 IP 地址(1)

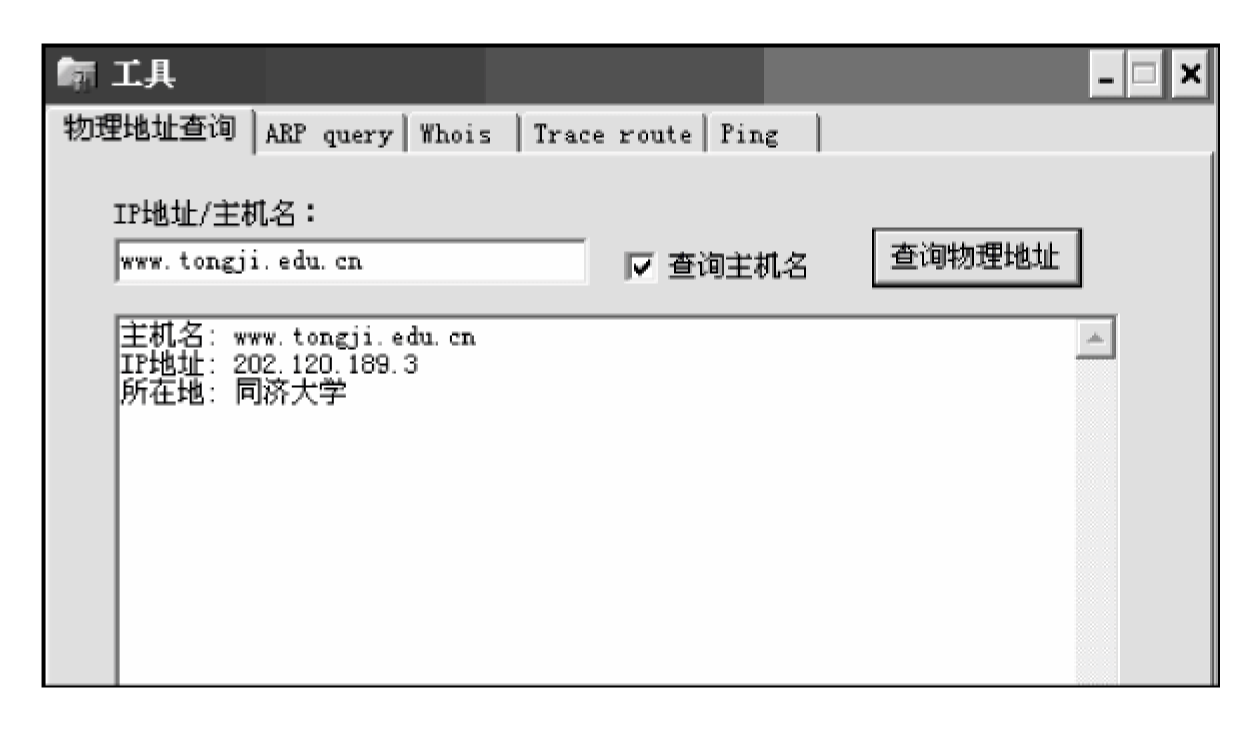


图 6.37　查询已知域名的 IP 地址(2)

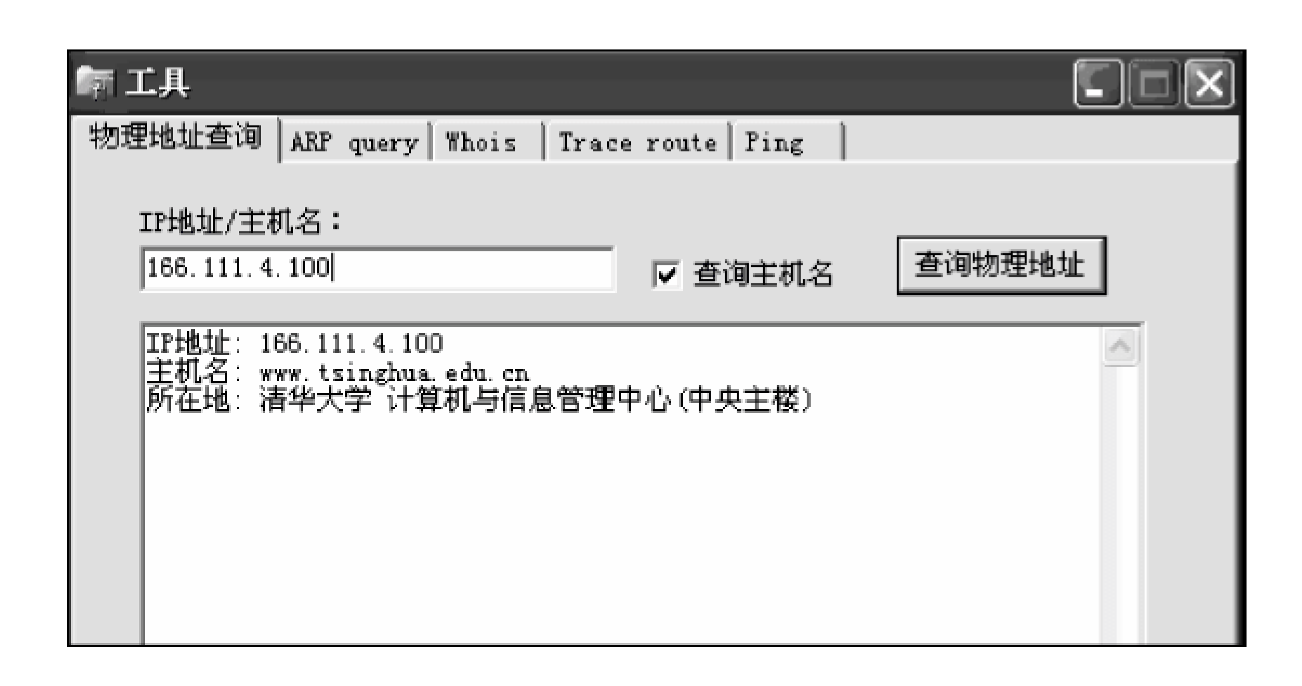


图 6.38　查询已知 IP 地址的域名(1)

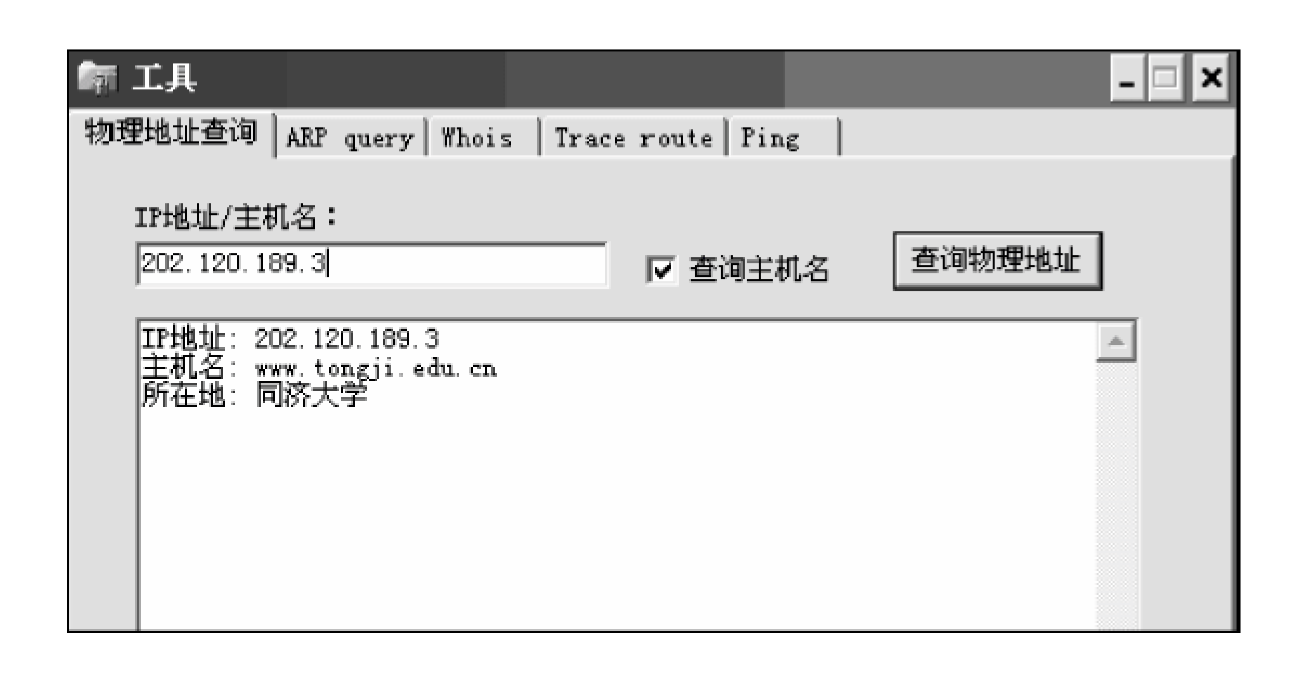


图 6.39　查询已知 IP 地址的域名(2)

4. 查询跟踪路由(trace route)

打开图 6.28 中的“工具”菜单，选择 Trace route，利用 X-Scan v3.3 可查询本机到指定主机的路由状况，如图 6.40 所示。本例为查询本机至清华大学主机的路径(Tracing route to www.tsinghua.edu.cn [166.111.4.100])。

由图 6.40 可知，两主机的路由过程中的部分 IP 地址的相应主机为 202.120.201.205 和 202.120.201.198，都是上海教育和科研计算机网的主机，202.112.36.253 和 202.112.46.57 都是北京市教育网信息中心的主机，59.66.2.1 和 59.66.2.18 分别是清华大学的 th002001.ip.tsinghua.edu.cn 和 th002018.ip.tsinghua.edu.cn 主机，166.111.4.100 为清华大学计算机与信息管理中心的 www.tsinghua.edu.cn 主机。

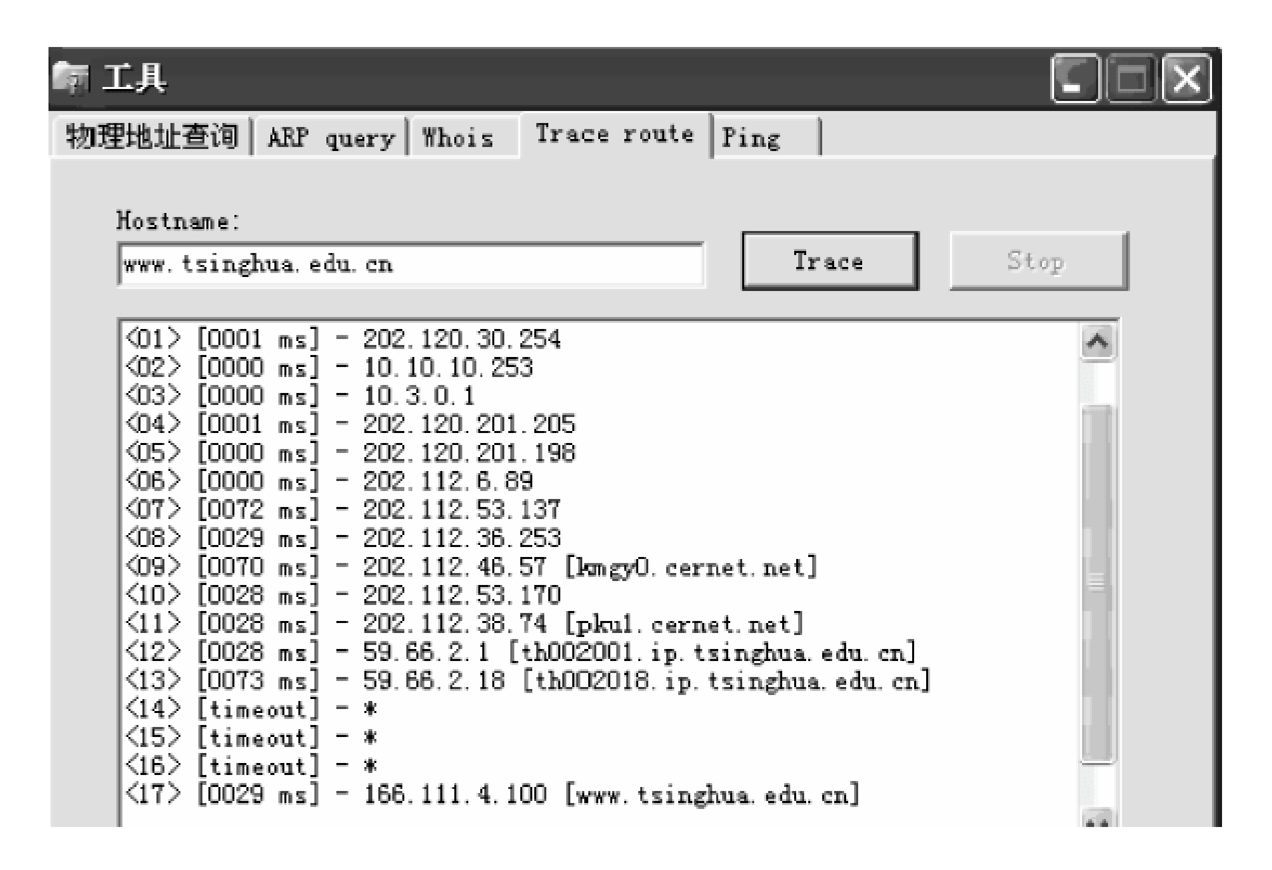


图 6.40 主机路由查询

5. 其他查询

打开图 6.22 中的“工具”菜单，选择 ARP query 选项，弹出如图 6.41 所示的窗口。在该窗口中，可查询到扫描范围内活动主机的 IP 地址的 MAC 地址。

此外，在此窗口还可以进行 Whois 查询和 Ping 检测。

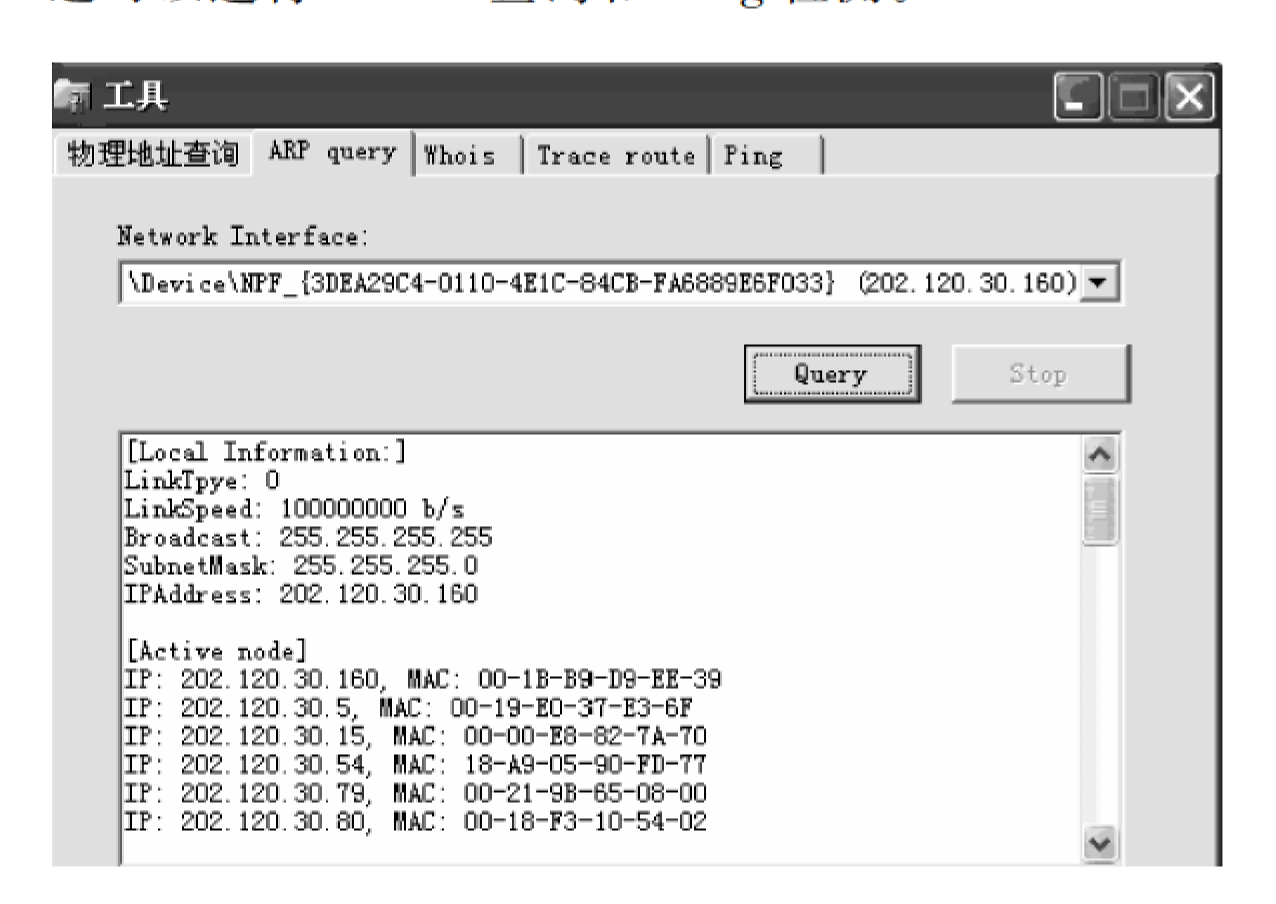


图 6.41 IP 地址和 MAC 地址查询

6.5.4 网络监听应用实例——数据包的捕获与分析

可以使用 Windows 自带的网络监视器程序，也可以使用专用的网络监视软件进行网络监听。通常专用的网络监视软件具有更强的数据捕获与过滤功能。

数据包的捕获就是通过技术手段截获网络中的数据包，并根据需要对数据包的内容进行过滤与分析，得到有价值的信息。这一技术被广泛应用于网络监控管理与网络信息刺探。在网络传输过程中，各种信息依据网络协议，逐级转换成电脉冲信号发送到传输介质上，在网络中的计算机接收到此脉冲信号后，由网卡内程序将脉冲还原成数据帧，并判读数据帧中的目的 MAC 地址。利用计算机上的网卡驱动程序设置的接收模式判断是否应该接收，若认为应该接收就将其接收并保存下来，然后交给操作系统处理；否则就丢弃不要。

现在广泛使用的局域网是以太网。在以太网中，同一个网段内的信息是以广播方式传播的。即在同一个网段内，一台主机发出的数据包可传向本网段的每一台主机。在以太网中，计算机间通信的必要条件有两个：第一，包含通信信息的电脉冲信号必须能到达接收信息主机的网络端口；第二，到达网络接口的数据包必须能够被网卡接受并交与操作系统。在正常通信情况下，上述第一点由网络中的路由器、交换机、集线器等设备及网络传输介质实现。这些设备可以保证将数据包按照数据包头部的目的地址传输到目的主机网卡上的网络端口；第二点由网卡上的处理电路、处理程序依据系统配置而实现。

1. Sniffer Portable 软件的功能

实现网络监听的工具软件有很多，各有特点。常用的网络监听软件有 Windows 网络监视器、Network Genral 公司的 Sniffer Portable 等。出于安全考虑，Windows 网络监视器仅允许捕获进出本机的数据包，禁止捕获与本机无关的主机间数据包；而 Sniffer Portable 是一款专用网络监视软件，可以捕获一切到达本机网络端口的数据包。现在介绍 Sniffer Portable 的应用。

Sniffer Portable 是功能强大的协议分析软件，可工作于 Windows 2000/XP 系统中。它以被动的方式监视和捕获每一个在网络中广播的数据包，并可对数据包的内容进行过滤、分析和存储。

Sniffer 产品服务中心网址是 http://www.sniffer-cn.com，如图 6.42 所示。该网站提供最新版本的 Sniffer Portable 软件免费下载服务，并提供 2 周的免费试用期。

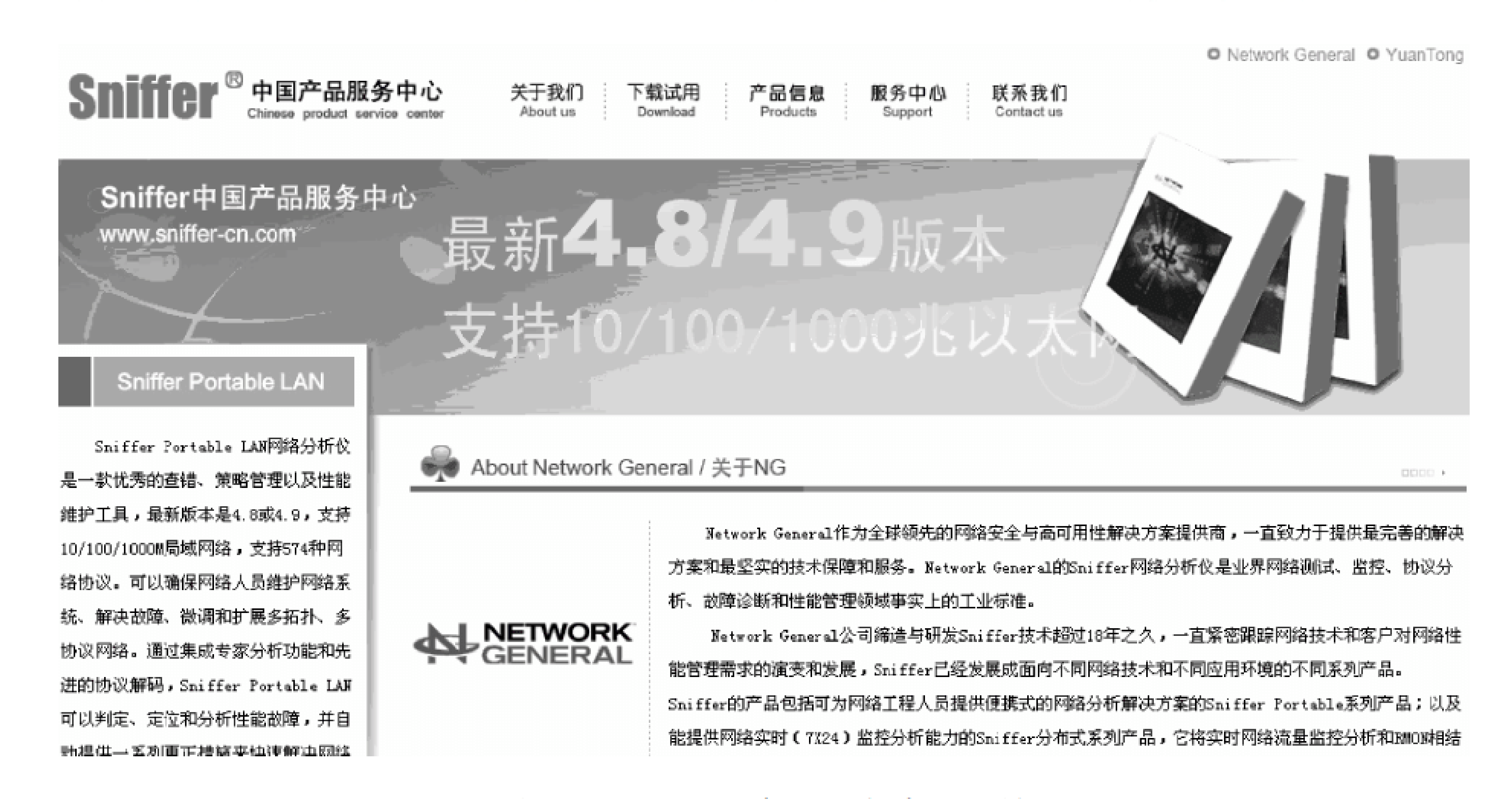


图 6.42　Sniffer 产品服务中心网站

对网络管理员来说，Sniffer 是一种强大的监控管理工具，可以分析网络中的协议、了解网络流量、发现异常通信等。对网络黑客而言，Sniffer 软件是一种重要的刺探工具，常被用来窃取网络账号和密码，窃取网络通信或电子邮件信息。因此说 Sniffer 软件也是一把双刃剑，可为网络管理工作提供重要的信息资源，也可为网络安全带来巨大的威胁。熟悉该软件可更好地管理网络，也可对 Sniffer Portable 带来的网络安全威胁进行有效的预防。Sniffer Portable 的主要功能如下：

- 对捕获的网络数据包进行详细分析。
- 利用专家分析系统诊断问题。
- 实时监控网络活动。
- 收集网络利用率和错误信息。

Sniffer Portable 主界面如图 6.43 所示。从图中可以看出 Sniffer Portable 软件主界面由菜单栏、工具栏、仪表板、状态栏等部分组成。仪表板上有带宽占用率、每秒封包数和差错率 3 个表盘，显示当前网络工作的状况。仪表板下面是网络图表，用曲线反映不同时刻网络工作的状况。

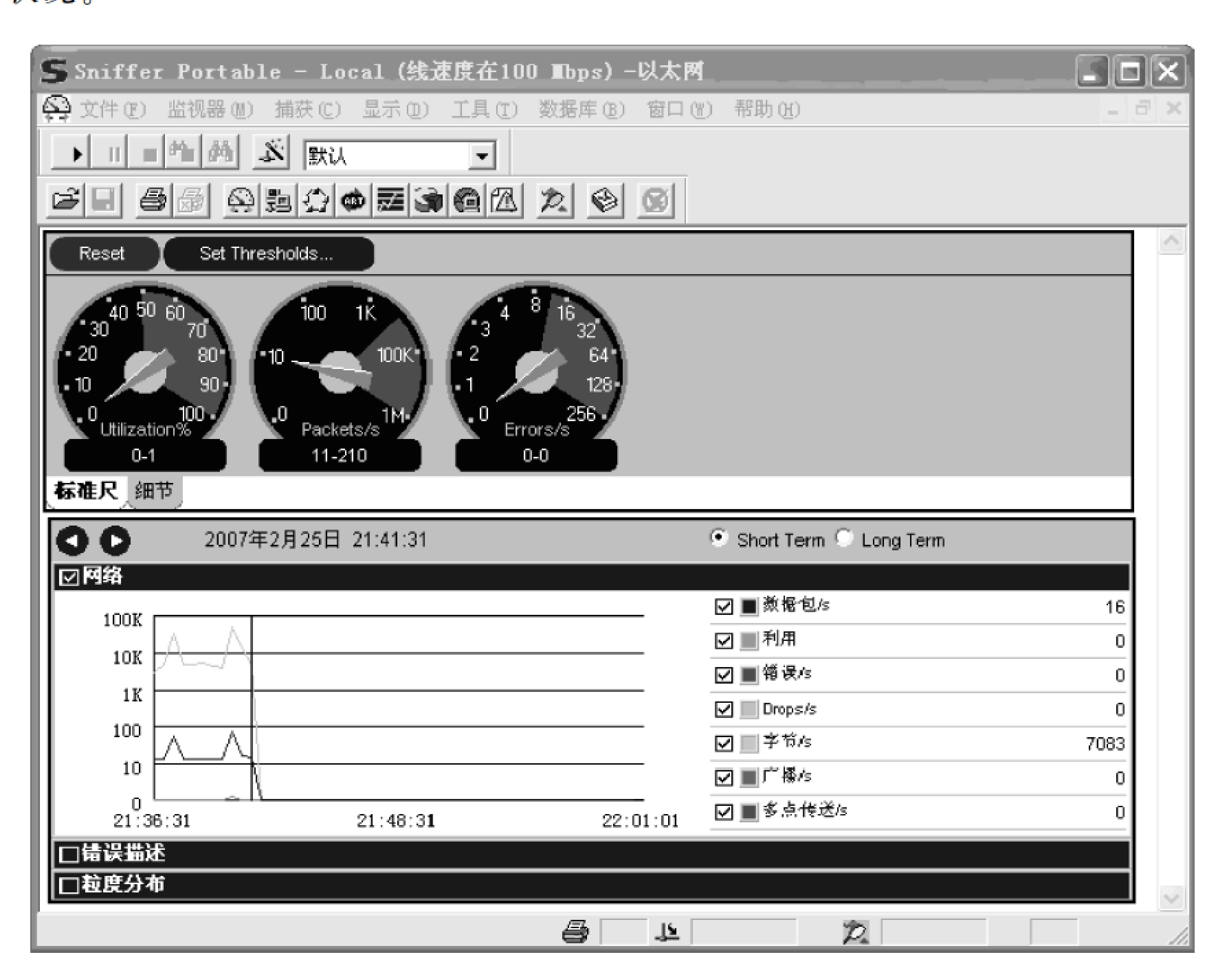


图 6.43　Sniffer Portable 软件主界面

Sniffer Portable 共有 7 个下拉菜单，其主要功能如下：

(1) 文件菜单

具有打开和保存各种记录数据文件、软件系统工作模式的设定、打印各种报表或报告和运行脚本程序等功能项。

(2) 监视器菜单

选择设定系统监视对象和监视的任务，可以定义过滤器对监视的对象有选择地做出显示，也可以查看报警日志。

(3) 捕获菜单

具有启动或停止捕获操作、按照不同的工作需求设置捕获过滤器和为捕获操作设置触发条件等功能项。这些功能可大大地提高捕获工作效率。

(4) 显示菜单

显示捕获数据的内容，并对显示内容进行搜索和过滤。

(5) 工具菜单

包含系统配置选项、监视对象地址簿和数据包自动发送等系统工具。

(6) 数据库菜单

对保存数据的数据库进行整理和维护。

(7) 窗口菜单

按不同的工作需要显示或隐藏不同的窗口。

在 Sniffer Portable 软件中，与网络安全密切相关的是信息捕获部分。

2. 数据包的捕获与过滤

Sniffer Portable 软件的安装与配置过程可参考相关的使用手册或实验指导资料，在此较详细地介绍该软件的应用。

(1) Sniffer Portable 的启动

Sniffer Portable 软件安装好后，选择“开始”→“程序”→Sniffer Pro 菜单，单击 Sniffer 启动 Sniffer Portable 程序，弹出如图 6.44 所示的“当前设置”对话框，对话框中列表显示出本计算机中可以使用的网卡。若计算机中装有多个网卡，需要从中选择准备用于监听的网卡，即选中与被监听系统连接的网卡，再单击“确定”按钮。



图 6.44　“当前设置”对话框

(2) 数据包的捕获

捕获数据包需要将监听主机与被监听主机通过集线器连接在一起。

Sniffer Portable 捕获工具栏共有“开始”、“暂停”、“停止”、“停止和显示”、“显示”和“定义过滤器”6 个按钮，如图 6.45 所示。



图 6.45　捕获工具栏

捕获方法很简单，单击捕获工具栏上的“开始”按钮即可开始捕获。一旦捕获到有效数据包，捕获工具栏上的“停止和显示”按钮由灰色变为彩色，单击此按钮可停止捕获并显示捕获数据包的内容。

(3) 数据包的读取与分析

Sniffer Portable 捕获到的数据包被暂存在内存里，单击“显示”或“停止和显示”按钮可以把捕获的数据包内容显示出来。在数据显示窗口中，通过窗口标签可以选择如下显示模式。

- 专家模式：该模式是一种综合显示模式，将各种捕获数据的信息综合排列显示在窗口中。
- 解码显示模式：该模式可将捕获到的数据依据不同的协议依次详细显示出来，是数

据分析的主要模式。在这种模式下，可以清晰地看到数据包中每一个字节内容及其在协议中所处的位置与含义，如图 6.46 所示。

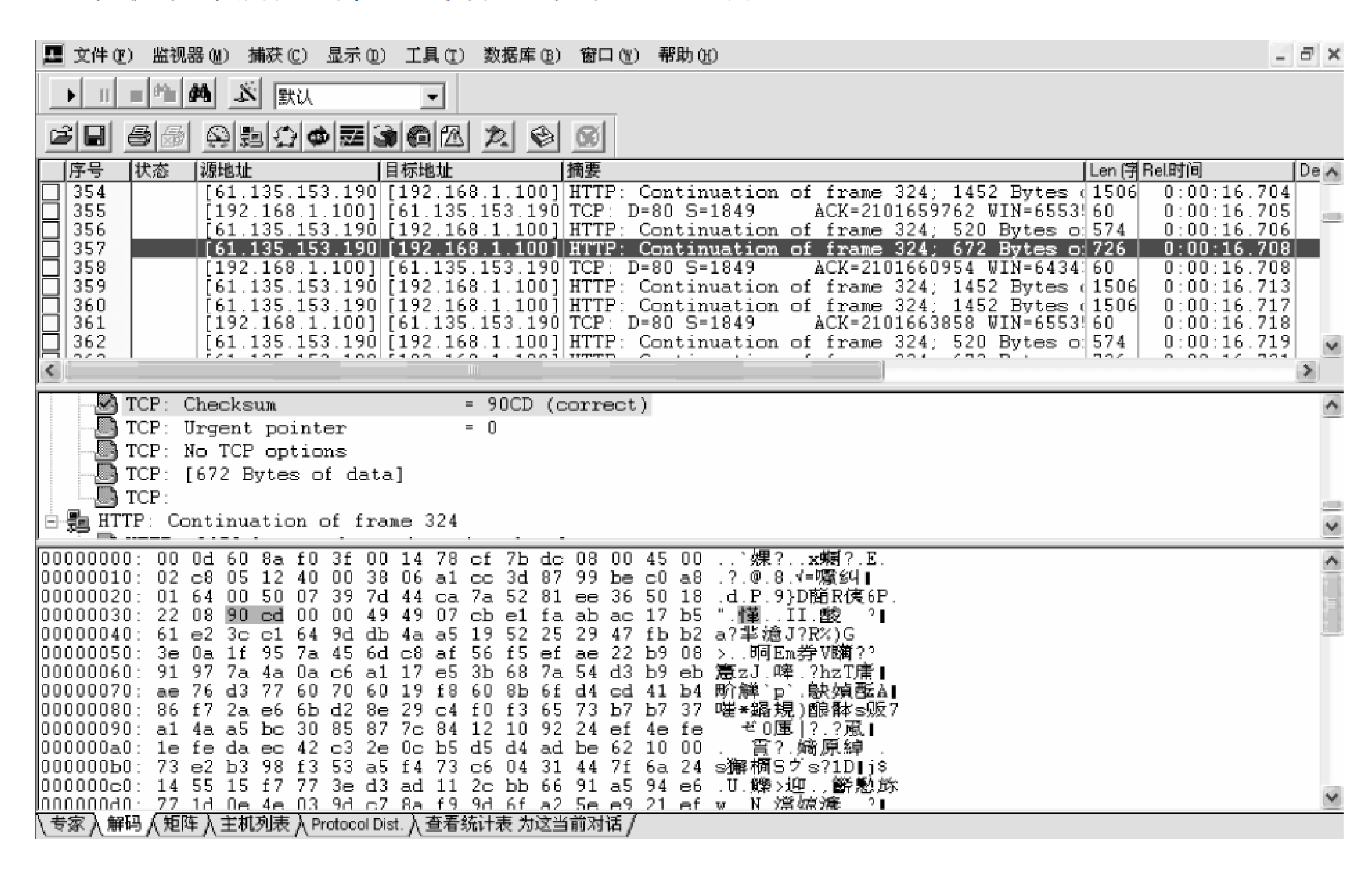


图 6.46 解码显示模式

- 矩阵显示模式：该模式可以直观地看出捕获的数据包中哪些地址的主机间进行了何种协议的连接。
- 主机列表显示模式：在该模式下详细列出每一个地址上各种协议出入数据包的数量及字节数。

(4) 捕获过滤

Sniffer Portable 的信息捕获能力很强，在瞬间可以捕获大量的数据，虽然其中有些数据是有价值的，但绝大多数数据是无用的，如果不对这些数据有选择地捕获，会占用大量的系统资源，而且会给提取有用信息带来困难。

Sniffer Portable 有着很强的数据过滤功能，通过合理配置过滤器，可以仅对有价值的信息进行捕获，提高系统工作效率，降低系统工作负荷。

单击 Sniffer Portable 捕获工具栏上的"定义过滤器"按钮，可以打开"定义过滤器"对话框。在对话框中可以设置按特定的地址及其数据传输方向进行过滤，如图 6.47 所示；可以设置按某种协议或数据包大小进行捕获，如图 6.48 所示；可以设置捕获缓冲区的大小，并设置自动将缓冲区内容保存到指定位置的文件中，如图 6.49 所示。



图 6.47 定义过滤器——地址



图 6.48　定义过滤器——高级

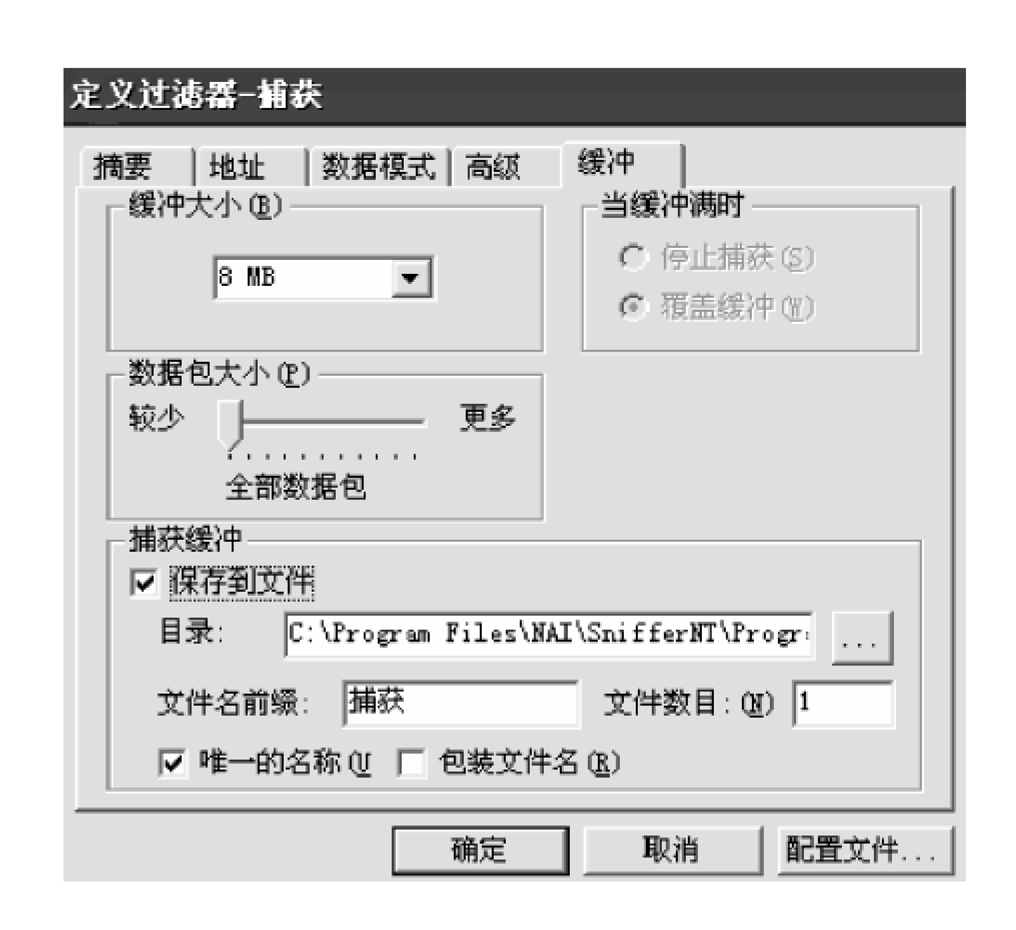


图 6.49　定义过滤器——缓冲

通过上面过滤条件的指定，可以有针对性地进行信息捕获，使捕获到的数据包所包含的都是所需要的信息。

3. 网络协议分析

捕获数据包的目的是获得网络中有价值的信息。在捕获了网络传输的数据包后，利用Sniffer Portable软件可以对捕获的数据按照不同的网络协议层进行分析与解释，可极大地方便对捕获到的数据进行分析和理解。

图6.50所示是在解码显示模式下使用Sniffer Portable软件捕获的一段网络通信内容。窗口工作区被分成三层窗格。上面的窗格显示数据包列表，每一行代表一个数据包，可以看到每一个数据包在这批数据中的编号、数据包源地址、目标地址和数据包内容摘要等；下面窗格显示当前选中的数据包用十六进制和ASCII码显示的具体内容；中间窗格显示当前选中的数据包中包含的网络协议和各协议报头在数据包中的位置。

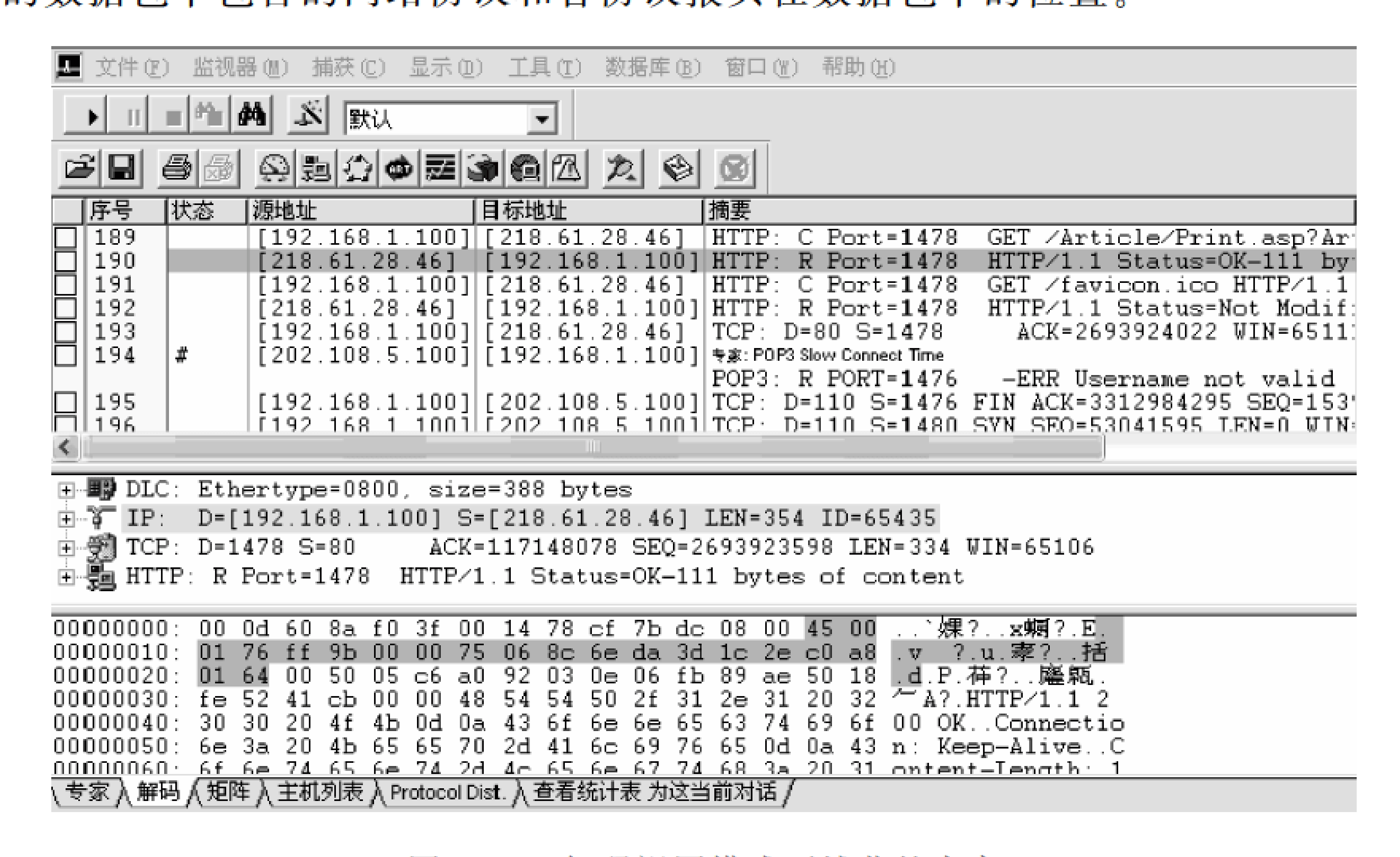


图 6.50　解码视图模式下捕获的内容

在下面窗格中用鼠标选中一个协议后，就会用灰色底纹突显出与协议相关的内容。

(1) DLC 帧分析

现在以 DLC(数据链路控制)帧为例，学习使用 Sniffer Portable 软件分析网络协议的方法。

在数据链路层，数据是以帧为单位进行发送的。以太网帧包含如下 6 个域：

① 前导：8 个字节，用于同步和起始标志，在 Sniffer Portable 中不显示。

② 目的地址：6 个字节，表示目的主机 MAC 地址。

③ 源地址：6 个字节，表示源主机 MAC 地址。

④ 类型域：2 个字节，标识在以太网上运行的客户端协议，如 IP、IPX 等网络层协议。

⑤ 数据域：46～1500 字节，这里是真正要传输的数据。如果长度少于 46 字节则由 DLC 协议自动填充到 46 字节。

⑥ 帧校验序列：4 个字节，利用 CRC 循环冗余校验法，在 Sniffer Portable 中不显示。

下面以如图 6.51 所示数据包实例分析 DLC 帧的结构，从图中可看到，此帧以 DLC Header 开头，帧内容包含 IP 和 TCP 协议内容。

```
DLC:  ----- DLC Header -----
  DLC:
  DLC:  Frame 217 arrived at  01:07:25.3184; frame size is 60 (003C hex) bytes.
  DLC:  Destination = Station 001478CF7BDC
  DLC:  Source      = Station 000D608AF03F
  DLC:  Ethertype   = 0800 (IP)
  DLC:
IP:  D=[202.108.5.100] S=[192.168.1.100] LEN=20 ID=51893
TCP: D=110 S=1480 FIN ACK=3318782200 SEQ=53041648 LEN=0 WIN=65378
DLC:  Frame padding= 6 bytes

00000000: 00 14 78 cf 7b dc 00 0d 60 8a f0 3f 08 00 45 00
00000010: 00 28 ca b5 40 00 80 06 9e 3d c0 a8 01 64 ca 6c
00000020: 05 64 05 c8 00 6e 03 29 59 f0 c5 d0 98 f8 50 11
00000030: ff 62 5c 7b 00 00 00 00 00 00 00 00              b\{........
```

图 6.51 DLC 帧结构

在 DLC 头部共显示 6 行信息，其中第 3～5 行显示内容是 DLC 的真实内容，其他行是 Sniffer Portable 添加的状态信息。

第 1 行：Sniffer Portable 添加的 DLC 起始标志。

第 2 行：Sniffer Portable 添加的帧序号、捕获日期、时间、帧的长度等信息。

以上 2 行内容在数据包中是没有的。

第 3 行：目标主机的 MAC 地址，占 6 个字节，帧内地址 00H～05H。

第 4 行：源主机的 MAC 地址，占 6 个字节，帧内地址 06H～0BH。

第 5 行：网络层协议的类型，占 2 个字节，帧内地址 0CH～0DH。IP 协议为 0800、ARP 协议为 0806 等。

第 6 行：Sniffer Portable 添加的 DLC 结束标志。

DLC 结束标志之后是此帧所要传输信息的真实内容。此帧内容包括 IP 和 TCP 协议两部分，其中 IP 协议内容长度为 20 字节。帧的最后一行是 DLC 填充段。因为此数据帧内容长度不足 46 字节，DLC 自动添加了 6 个字节的 00 将其补足为 46 字节。

(2) IP 数据包分析

IP 报头从数据包中第 0EH 字节开始(00H～0DH 是 DLC 帧头)，如图 6.52 所示。

```
IP: ----- IP Header -----
  IP:
  IP: Version = 4, header length = 20 bytes
  IP: Type of service = 00
  IP:       000. ....  = routine
  IP:       ...0 .... = normal delay
  IP:       .... 0... = normal throughput
  IP:       .... .0.. = normal reliability
  IP:       .... ..0. = ECT bit - transport protocol will ignore the CE bit
  IP:       .... ...0 = CE bit - no congestion
  IP: Total length    = 82 bytes
  IP: Identification  = 30970
  IP: Flags           = 4X
  IP:       .1.. .... = don't fragment
  IP:       ..0. .... = last fragment
  IP: Fragment offset = 0 bytes
  IP: Time to live    = 51 seconds/hops
  IP: Protocol        = 6 (TCP)
  IP: Header checksum = F1E3 (correct)
  IP: Source address      = [219.133.63.54]
  IP: Destination address = [192.168.1.100]
  IP: No options
  IP:
TCP: D=3801 S=80     ACK=2630515208 SEQ=809852913 LEN=42 WIN=8712
00000000: 00 0d 60 8a f0 3f 00 14 78 cf 7b dc 08 00 45 00  ..`婐?..x蝲?.E.
00000010: 00 52 78 fa 40 00 33 06 f1 e3 db 85 3f 36 c0 a8  .Rx鷃.3.襁踝?6括
00000020: 01 64 00 50 0e d9 30 45 5f f1 9c ca 7a 08 50 18  .d.P.?E_駧蕄.P.
00000030: 22 08 6c 1c 00 00 00 2a 02 10 1f 00 02 16 32 d9  ".l....*......2
00000040: 4a 60 6f 44 9c af 54 c7 e0 10 06 45 b5 ce a2 0c  J`oD湇T青..E滴?
00000050: fd 88 53 d6 35 1d 99 4a dc a5 6d 91 0c 0b d9 03  龍S?.櫃堀m?.?
```

图 6.52　数据包中的开始字节

地址 0E 占 1 字节，其中高 4 位是 IP 协议版本号，低 4 位是本包 IP 首部长度。此例中 0EH 地址内容为 45H，IP 协议版本号为 4(即 IPv4)，此包所经过的各个路由器等网络设备均按 IPv4 格式对数据包进行解读与处理；数据包 IP 首部长度为 20 字节。

地址 0F 占 1 字节，表示服务类型。定义 IP 协议包的处理方法，包含 3 位过程字段，1 位延迟字段，1 位流量字段，1 位可靠性字段，1 位成本字段和 1 位未用字段。

地址 10H～11H 占 2 字节，表示 IP 包总长度。此例中 IP 包总长度为 0052H，即 82 字节；从 0EH 到 5FH 包含了 IP 包头及数据长度。

地址 12H～13H 占 2 字节，表示 IP 报文标识字段，每一个 IP 数据包都有一个与分组过程相关的唯一标识，作为到达目标后恢复数据时组合的依据。此例中标识为 78FAH。

地址 14H～15H 占 2 字节，高 3 位是有关数据分段的标识，低 13 位是段偏移。当数据分组时，它和更多段位进行连接，帮助目的主机将分段的包组合。

地址 16H 占 1 字节，表示 IP 包生存时间(TTL)。当某一网络设备发出 IP 包的同时要给 IP 包设定一个生存时间常数，每经过一个路由器此时间常数自动减 1，当 TTL 值减为 0 还无法找到目标主机时就自动消亡。此例中捕获到的数据包 TTL 值为 33H(51)，表明它从发出到被捕获已经过 64－51＝13 个路由器了。

地址 17H 占 1 字节，是协议代码，表示此 IP 包携带的是何种协议报文。常见的有 ICMP、TCP 和 UDP。此例中协议代码值为 6，表示报文是 TCP 协议。

地址 18H～19H 占 2 字节，表示首部校验和，用于校验和纠错。

地址 1AH～1DH 占 4 字节，表示源 IP 地址。此例为 DBH、85H、3FH 和 36H 4 字节，用点分十进制表示即为 219.133.63.54。

地址 1EH～21H 占 4 字节，表示目标 IP 地址。此例为 C0H、A8H、01H 和 64H 4 字

节，用点分十进制表示即为 192.168.1.100。

随后是选项，此例中没有选项。选项之后是此 IP 数据包的载荷。此例为 TCP 协议传输的数据。

(3) ARP 数据包结构分析

如图 6.53 所示是 IP 地址为 192.168.1.100 的主机向 IP 地址为 192.168.1.101 的主机发出 ARP 请求的数据包。

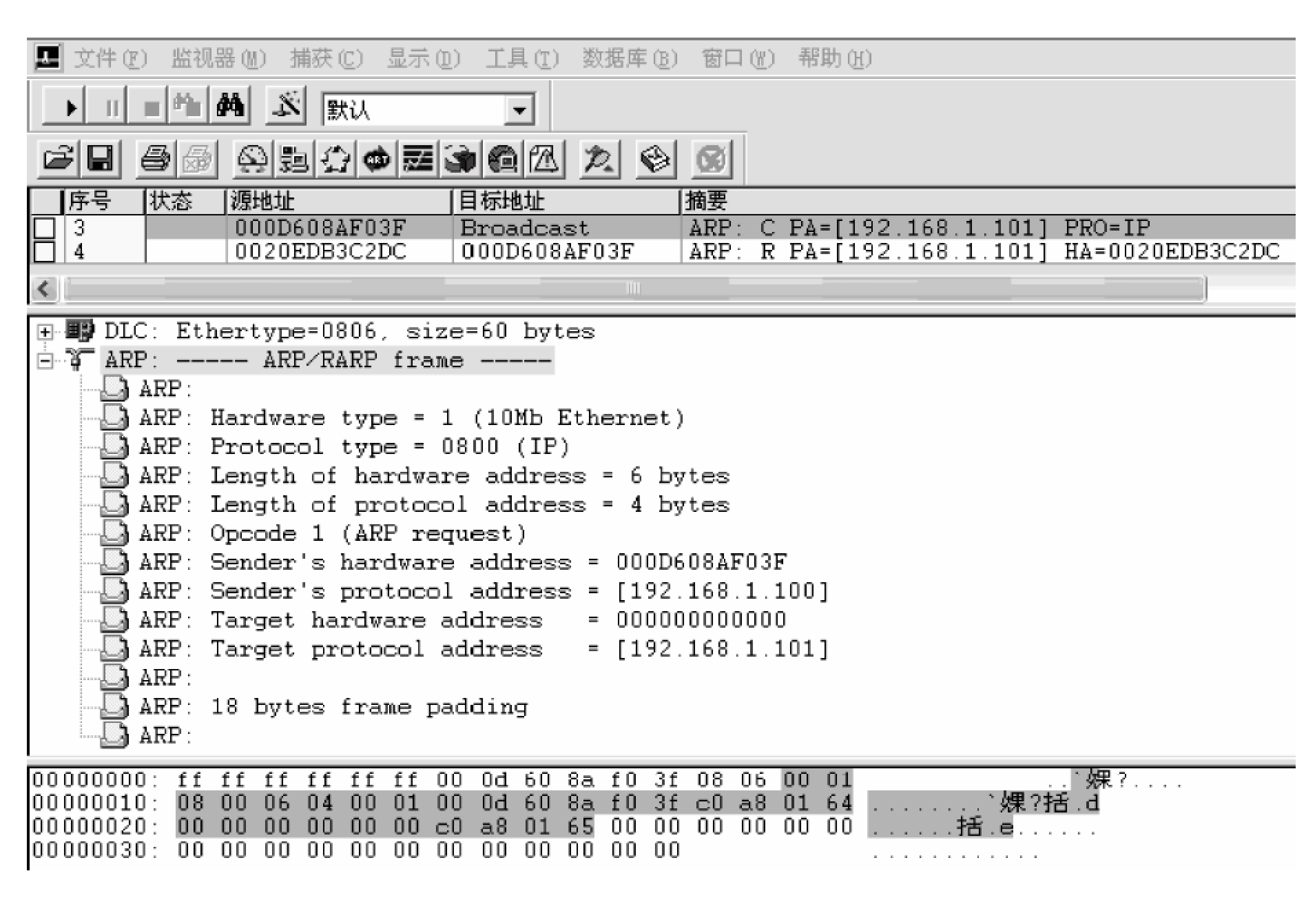


图 6.53 ARP 请求的数据包

数据包前 14 个字节为 DLC 包头，ARP 协议包从偏移地址 0EH 开始到 29H 结束。

地址 0EH～0FH 表示硬件类型，以太网为 0001H。

地址 10H～11H 表示网络层协议类型，IP 协议为 0800。

地址 12H 表示硬件地址长度，MAX 地址长度恒为 6 字节。

地址 13H 表示协议地址长度，IP 地址恒为 4 字节。

地址 14H～15H 表示操作，请求包恒为 1，应答包恒为 2。此例是请求包，值为 1。

地址 16H～1BH 表示源主机的 MAC 地址。此例为 00-0D-60-8A-F0-3F。

地址 1CH～1FH 表示源主机协议地址。此例为 192.168.1.100，即 C0H、A8H、01H、64H。

地址 20H～25H 表示目标主机 MAC 地址。此例为 ARP 请求包，地址为 0。

地址 26H～29H 表示目标主机协议地址。此例为 192.168.1.101，即 C0H、A8H、01H、65H。

地址 2AH～3BH 为填充(DLC 将数据包不足长度部分补足)。

目标主机收到此 ARP 请求包后，回应一个 ARP 应答包，如图 6.54 所示。具体内容的含义请读者自己分析。

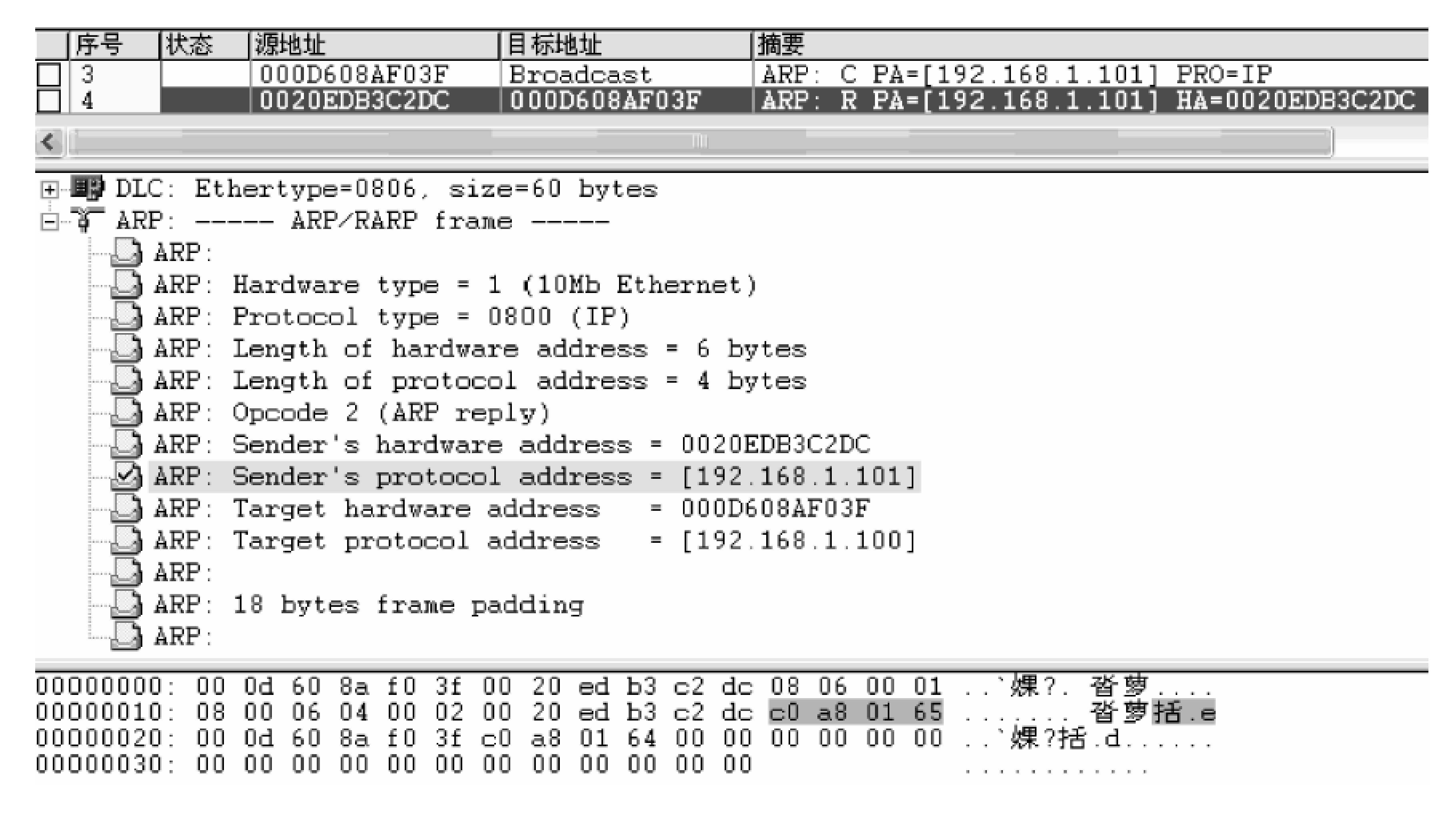


图 6.54　ARP 应答包内容

（4）ICMP 数据包结构分析

图 6.55 所示为使用 Sniffer Portable 捕获的一个 ICMP 数据包内容。

```
序号 状态 源地址            目标地址           摘要              Len(字 Rel.时间
1    M    [192.168.1.100] [202.108.33.32]  ICMP: Echo        74    0:00:00.000
2         [202.108.33.32] [192.168.1.100]  ICMP: Echo reply  74    0:00:00.028
3         [192.168.1.100] [202.108.33.32]  ICMP: Echo        74    0:00:01.005
4         [202.108.33.32] [192.168.1.100]  ICMP: Echo reply  74    0:00:01.017
5         [192.168.1.100] [202.108.33.32]  ICMP: Echo        74    0:00:02.006
6         [202.108.33.32] [192.168.1.100]  ICMP: Echo reply  74    0:00:02.020
7         [192.168.1.100] [202.108.33.32]  ICMP: Echo        74    0:00:03.007
8         [202.108.33.32] [192.168.1.100]  ICMP: Echo reply  74    0:00:03.050

DLC: Ethertype=0800, size=74 bytes
IP:  D=[202.108.33.32] S=[192.168.1.100] LEN=40 ID=10981
ICMP: ----- ICMP header -----
ICMP:
ICMP: Type = 8 (Echo)
ICMP: Code = 0
ICMP: Checksum = 495C (correct)
ICMP: Identifier = 768
ICMP: Sequence number = 256
ICMP: [32 bytes of data]
ICMP:
ICMP: [Normal end of "ICMP header".]
ICMP:

00000000: 00 14 78 cf 7b dc 00 0d 60 8a f0 3f 08 00 45 00
00000010: 00 3c 2a e5 00 00 80 01 62 43 c0 a8 01 64 ca 6c
00000020: 21 20 08 00 49 5c 03 00 01 00 61 62 63 64 65 66   !  ..I\....abcdef
00000030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76   ghijklmnopqrstuv
00000040: 77 61 62 63 64 65 66 67 68 69                     wabcdefghi

专家 解码 矩阵 主机列表 Protocol Dist. 查看统计表 为这当前对话
```

图 6.55　捕获的 ICMP 数据包内容

地址 00H～0DH 为 DLC 包头；0EH～21H 为 IP 包头。

地址 22H 为 ICMP 数据包类型字段，不同的代码代表此数据包不同的类型。此例中代码为 08，类型描述为响应请求。

地址 23H 为代码，前 1 字节设定的类型不同，此字节含义也不同。此例中为 0。

地址 24H～25H 为校验和，用于校验数据包的正确性。

以下内容随不同的类型和代码有不同的数据内容。此例为响应请求 ICMP 包，其内

容为：

地址 26H～27H 为标识。

地址 28H～29H 表示发送的二进制位序列号。

地址 2AH～49H 为发送探测包内容。使用 Windows 系统的 ping 命令时内容为英文小写字母 a～w 循环发送，直至达到命令要求的字节数为止，默认字节数为 32。

图 6.56 为上述响应请求的应答包，内容读者自己分析。

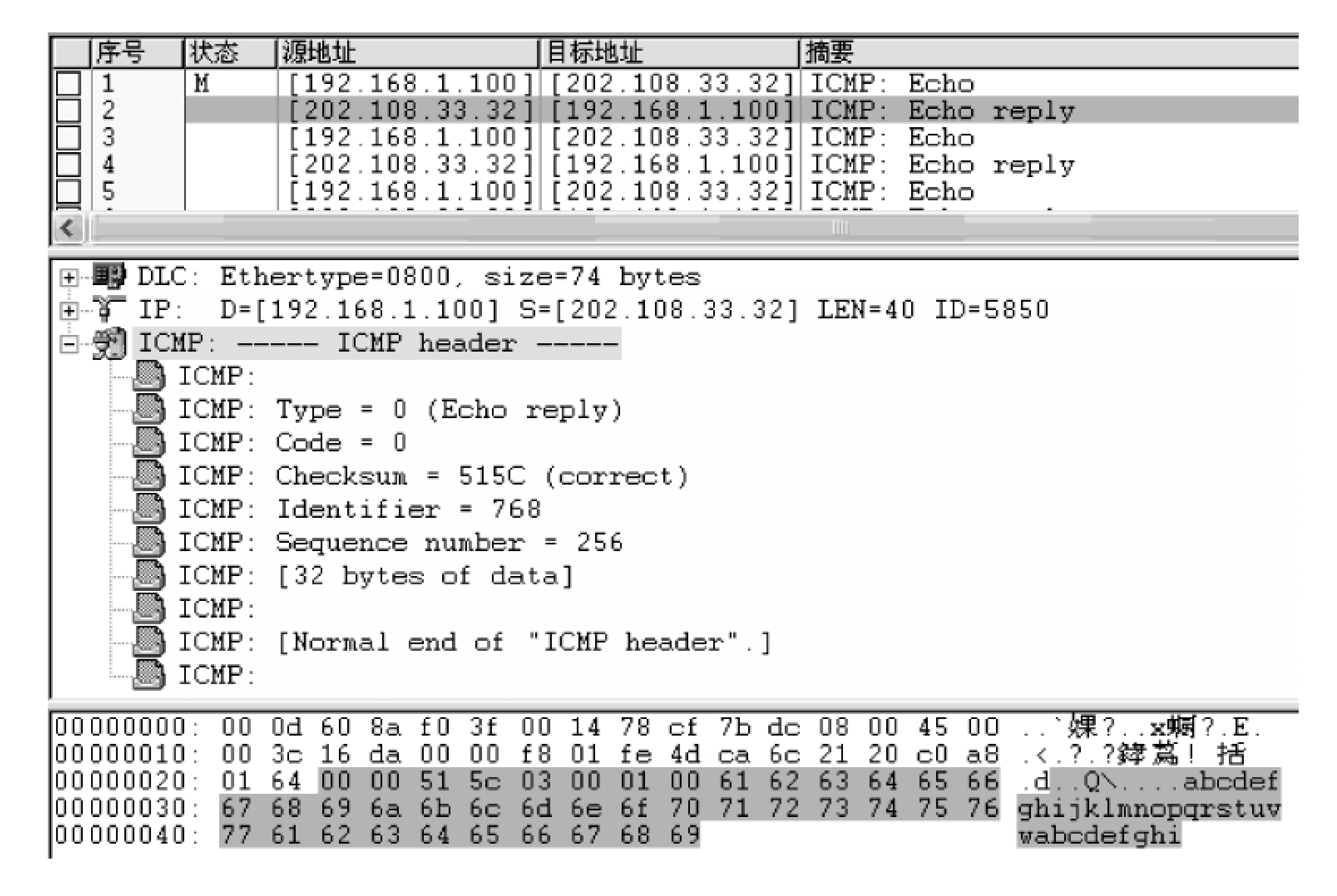


图 6.56　ICMP 响应请求应答包

（5）TCP 数据包结构分析

图 6.57 为 TCP 数据包结构，分析如下：

地址 00H～0DH 为 DLC 包头；0EH～21H 为 IP 包头。

地址 22H～23H 表示源主机端口号。此例为使用 HTTP 协议访问网页，默认端口号为 80(0050H)。

地址 24H～25H 表示目标主机端口号，由应用程序随机产生。此例为 3545(0DD9H)。

地址 26H～29H 为序号，指明段在即将传输的段序列中的位置。此例中序号为 2938112427(AF2009ABH)。

地址 2AH～2DH 为确认号，作为收到数据的响应，连接成功后传输数据过程中此号为请求包序号＋应答数据包长度，若不进行通信仅进行连接时长度为 1 字节(同步字节)。此例为 648 543 792＋1＝648 543 793(26A7FE31H)。

地址 2EH 的高 4 位为首部长度，其值为首部字节数/4；低 4 位保留未用。此例 TCP 首部长度 20 字节，故此字节高 4 位值＝20/4＝5。

地址 2FH 的高 2 位保留未用；低 6 位为标志位。

地址 30H～31H 为指定发送端能传输下一段大小的窗口。此例为 65259(FEEBH)。

地址 32H～33H 为用来校验段头和数据部分可靠性的校验和。此例为 082DH。

地址 34H～35H 为段中包含的紧急信息，只有当 URG 标志置 1 时紧急指针才有效。此例为 0。

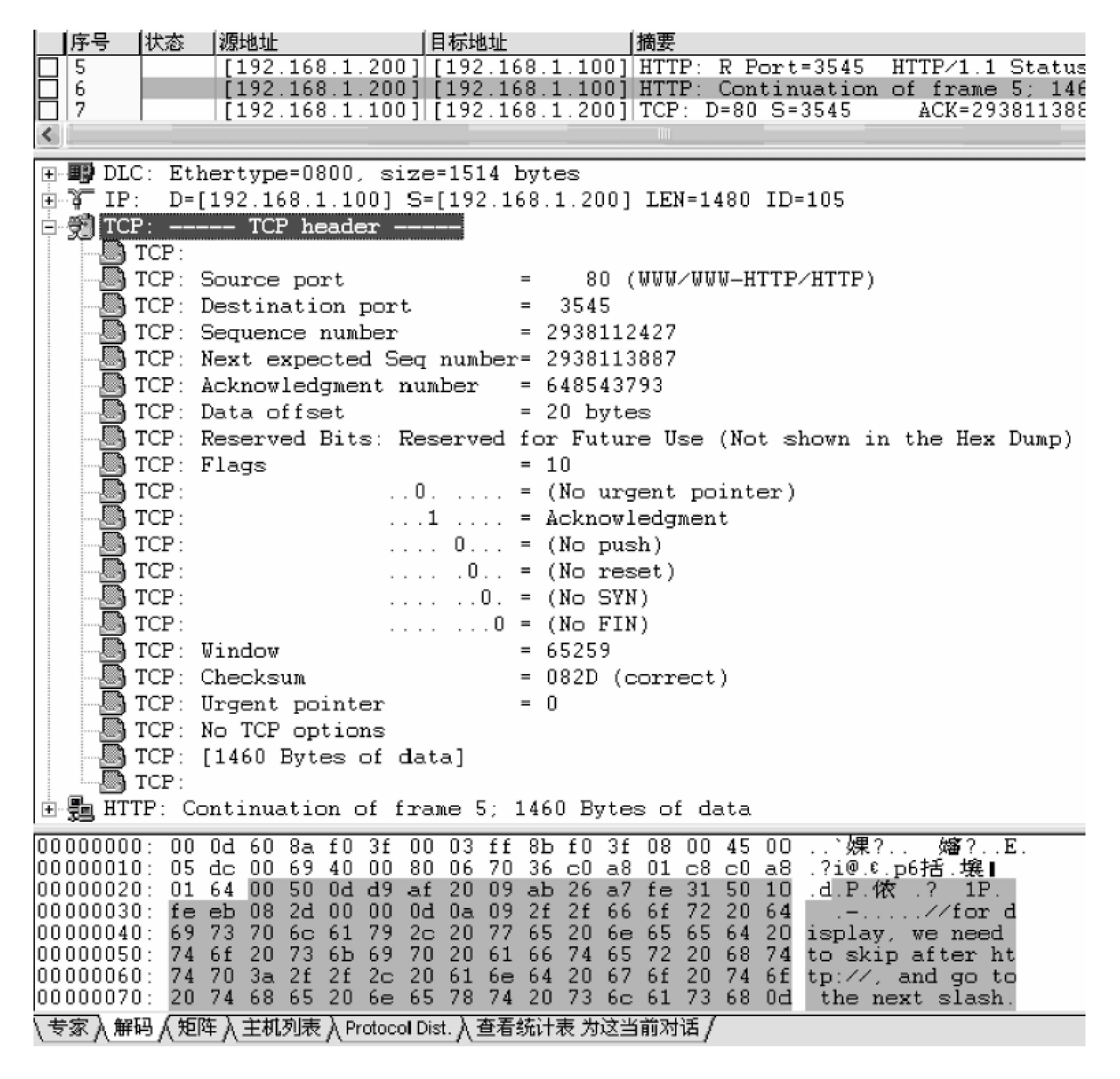


图 6.57　TCP 数据包结构

以下地址若有选项则为连续 32 字节选项。此例没有选项字段。后面内容全部为被传输的数据。此例为以 HTTP 协议传输的超文本网页信息，全部以明文方式传输。

4. 数据的安全问题

网络中的数据通常采用明码传送的，任何人只要将数据包捕获，就可以很容易地获得数据包中的信息。而通过以上介绍可知，在网络中信息传输是很容易被捕获和分析的，这样会给网络数据的安全性带来威胁。

在捕获的数据包中可以了解到通信双方的 IP 地址、主机物理地址、使用的通信协议、登录账户和密码以及通信内容等。

图 6.58 是一个被捕获的数据包，从图中数据内容可以看到通信双方计算机的 IP 地址分别为 192.168.1.100 和 202.108.37.68，双方的物理地址分别是 001478CF7BDCH 和 000D608AF03FH，使用 HTTP 协议浏览网页，网页的内容是有关人大和政协会议等。

通过 Sniffer Portable 可以很容易了解到各个主机上的信息流量、各主机访问或被访问的状态，从中可以刺探到业务内容和业务量等商业敏感信息。

黑客利用协议实现的攻击，都是故意错误地设定数据包头的一些重要字段，使接收端在把收到的数据组装成一个完整数据包的过程中出现错误，这样的错误往往会造成系统宕机或系统崩溃。通过以上分析可以看到，黑客的网络嗅探是对网络安全的重大威胁，因此，网络管理员必须采取相应的措施及时发现并阻止。

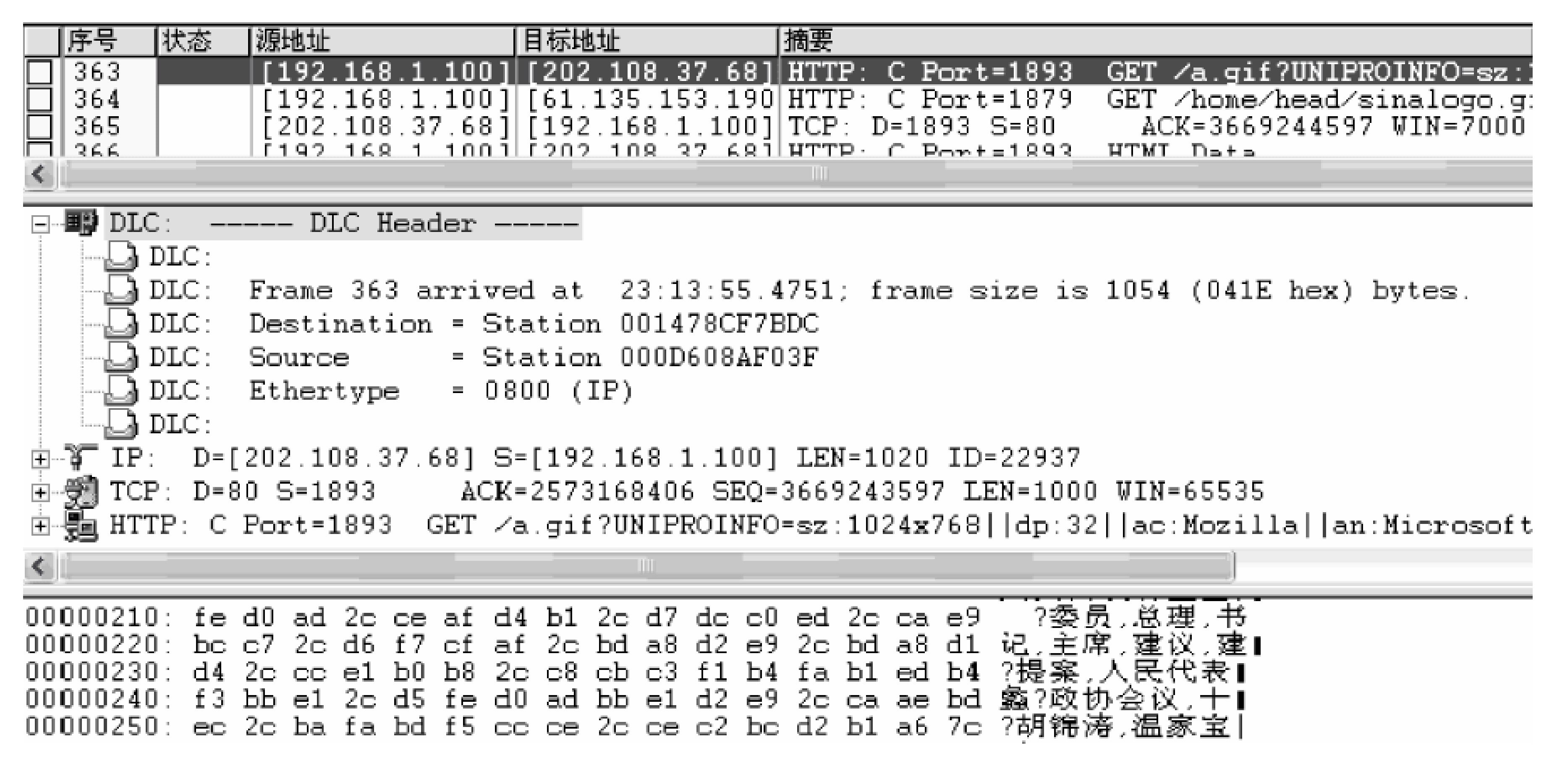


图 6.58 捕获的数据包实例

习题和思考题

一、问答题

1. 什么是防火墙？防火墙的主要功能和技术有哪些？
2. 什么是计算机病毒？计算机病毒有哪些特征？什么是计算机网络病毒？
3. 简述木马和蠕虫的特点和危害。
4. 什么是黑客？简述黑客攻击的主要类型、攻击的手段和工具。
5. 简述黑客攻击的过程。
6. 什么是入侵检测系统？简述入侵检测系统和防护系统的功能。
7. 什么是网络系统漏洞？网络系统漏洞主要表现在哪几个方面？
8. 什么是网络扫描和网络监听？什么样的用户可以进行网络扫描和网络监听？
9. 说出几种你熟悉或使用的防病毒软件、网络扫描软件和网络监听软件。

二、填空题

1. 网络病毒具有传播方式复杂、(　　)、(　　)和破坏危害大等特点。
2. 防范病毒主要从(　　)和(　　)两方面入手。
3. 常用的防火墙技术有(　　)技术、(　　)技术、(　　)技术和自适应代理技术。
4. 代理服务程序在幕后处理所有(　　)和(　　)之间的通信以代替相互间的直接交谈。
5. 黑客进行的网络攻击通常可分为(　　)型、(　　)型和(　　)型攻击。
6. (　　)攻击是指通过向程序的缓冲区写入超出其长度的内容，从而破坏程序的堆栈，使程序转而执行其他的指令，以达到攻击的目的。
7. (　　)攻击是攻击者通过各种手段来消耗网络带宽或服务器系统资源，最终导致被攻击服务器资源耗尽或系统崩溃而无法提供正常的网络服务。
8. IDS 是一种(　　)的安全防护措施，而 IPS 是一种(　　)的安全防护措施。
9. 网络系统硬件的缺陷主要有(　　)、(　　)、(　　)和存储介质脆弱等方面。

10. 网络系统的软件漏洞可分为(　　)、(　　)、数据库系统漏洞、(　　)和网络软件及网络服务漏洞。

三、单项选择题

1. 网络病毒不具有(　　)特点。

A. 传播速度快　B. 清除难度大　C. 传播方式单一　D. 破坏危害大

2. (　　)是一种基于远程控制的黑客工具,它通常寄生于用户的计算机系统中,盗窃用户信息,并通过网络发送给黑客。

A. 文件病毒　B. 木马　C. 引导型病毒　D. 蠕虫

3. 将防火墙软件安装在路由器上,就构成了简单的(　　)防火墙。

A. 包过滤　B. 子网过滤　C. 代理服务器　D. 主机过滤

4. 不管是什么种类的防火墙,都不能(　　)。

A. 强化网络安全策略　B. 对网络存取和访问进行监控审计

C. 保护内部网的安全　D. 防范绕过它的连接

5. (　　)是一种可以自我复制的完全独立的程序,它的传播不需要借助被感染主机的其他程序。它可以自动创建与其功能完全相同的副本,并在没人干涉的情况下自动运行。

A. 文件病毒　B. 木马　C. 引导型病毒　D. 蠕虫

6. 端口扫描也是一把双刃剑,黑客进行的端口扫描是一种(　　)型网络攻击。

A. DoS　B. 利用　C. 信息收集　D. 缓冲区溢出

7. (　　)攻击是一种特殊形式的拒绝服务攻击,它采用一种分布、协作的大规模攻击方式。

A. DoS　B. DDoS　C. 缓冲区溢出　D. IP 电子欺骗

8. 入侵防护系统的缩写是(1)(　　),(2)(　　)是认证中心,而(3)(　　)是入侵检测系统的缩写。

(1) A. IDS　B. IPS　C. CERT　D. CA

(2) A. IDS　B. IPS　C. CERT　D. CA

(3) A. IDS　B. IPS　C. CERT　D. CA

9. 在网络安全领域,网络系统"漏洞"是指网络系统硬件、软件或策略上存在的缺陷或脆弱性。网络系统(1)(　　)主要有硬件故障、网络线路威胁、电磁辐射和存储介质脆弱等方面;各种存储器中存储大量的信息,这些(2)(　　)很容易被盗窃或损坏,造成信息的丢失。

(1) A. 硬件方面的漏洞　B. 软件方面的漏洞　C. 硬件故障　D. 存储介质

(2) A. 硬件方面的漏洞　B. 软件方面的漏洞　C. 硬件故障　D. 存储介质

10. 网络系统的(1)(　　)通常有硬盘故障、电源故障、芯片主板故障、驱动器故障等;(2)(　　)也面对各种威胁,非法用户可对其进行物理破坏、搭线窃听、通过未保护的外部线路访问系统内部信息等。

(1) A. 电源故障　B. 通信线路　C. 硬件故障　D. 存储介质

(2) A. 电源故障　B. 通信线路　C. 硬件故障　D. 存储介质

四、实验题

1. 杀毒软件应用实验:下载、安装一个著名的计算机病毒杀毒软件,并熟练运用该软

件查杀病毒。

2．防火墙应用实验：下载、安装一个实用的网络防火墙软件（如天网防火墙），设置相关的限制条件，熟练运用该软件保护网络客户端。

3．IDS应用实验：下载、安装一个实用的网络IDS软件工具，并熟练运用该软件进行网络安全检测。

4．网络扫描器软件应用实验：下载、安装一个实用的网络扫描器软件（如NetToolsX、X-Scan），并熟练运用该软件进行网络安全扫描检测。

第7章 VPN安全技术与应用实践

虚拟专用网(virtual private network,VPN)是指依靠Internet服务提供者(ISP)和其他网络服务提供者(NSP)在公用网络中建立的专用数据通信网络。

VPN可使用户利用公用网的资源将分散在各地的机构动态地连接起来,进行数据低成本的安全传输,这样既节省长途电话费用支出,又不再需要专用线路。VPN是由物理上分布在不同地点的网络通过公用网络连接构成的逻辑上的虚拟子网,并采用认证、访问控制、数据的保密性和完整性等安全措施,使得数据通过安全的"加密管道"在公用网络中传输。这里的公用网通常是指Internet。

7.1 VPN技术基础

VPN是通过一个公用网络(通常是Internet)建立一个临时的、安全的连接,是对企业内部网的扩展。VPN可以实现不同网络的组件和资源之间的相互连接,它能够利用Internet或其他公共互联网络的基础设施为用户创建隧道,并提供与专用网络一样的安全和功能保障。

7.1.1 VPN概述

VPN技术实现内部网信息在公用信息网中的传输,就如同在茫茫的广域网中为用户拉出一条专线一样。VPN对用户端是透明的,用户好像使用一条专用线路在客户计算机和企业服务器之间建立点对点连接,进行数据的传输。VPN允许远程通信方、销售人员或企业分支机构使用Internet等公用网络的路由基础设施以安全的方式与位于企业局域网端的企业服务器建立连接。对用户来说,公用网络起到了"虚拟专用"的效果,通过VPN,网络对每个使用者都是"专用"的。使用VPN技术可以解决在当今远程通信量日益增大、企业全球运作广泛分布的情况下,员工需要访问企业网资源,企业相互之间必须进行及时和有效的通信问题。

1. VPN的功能

VPN技术同样支持企业通过Internet等公用网络与分支机构或其他公司建立连接,进行安全通信。这种跨越Internet建立的VPN连接逻辑上等同于两地之间使用广域网建立的连接。虽然VPN通信建立在公用网络基础上,但是用户在使用VPN时感觉如同在使用

专用网络进行通信一样。

VPN 使用经过身份验证的链接以确保只有授权用户才可以连接到网络，而且可使用加密来确保其他人无法截获或使用通过 Internet 传送的数据。Windows XP 使用点对点隧道协议（PPTP）或第二层隧道协议（L2TP）实现安全性。隧道协议是一项使 Internet 上从一台计算机到另一台计算机的信息传输更加安全的技术。

一般来说，企业在选用一种远程网络互联方案时都希望能够对访问企业资源和信息的要求加以控制。所选用的方案应当既能够实现授权用户与企业局域网资源的自由连接和不同分支机构之间的资源共享，又能够确保企业数据在公用网络或企业内部网络上传输时安全性不受破坏。因此，一个成功的 VPN 方案应具有以下方面的功能。

（1）用户验证

VPN 方案必须能够验证用户身份并严格控制只有授权用户才能访问 VPN。另外，方案还必须能够提供审计和计费功能，显示何人在何时访问了何种信息。

（2）地址管理

VPN 方案必须能够为用户分配专用网络上的地址并确保地址的安全性。

（3）数据加密

对通过公用网络传输的数据进行加密，确保网络其他未授权的用户无法读取该信息。

（4）密钥管理

VPN 方案必须能够生成并更新客户端和服务器的加密密钥。

（5）多协议支持

VPN 方案必须支持公用网络上普遍使用的基本协议。以 PPTP 或 L2TP 协议为基础的 VPN 方案既能够满足以上所有的基本要求，又能充分利用遍及世界各地的 Internet 优势。其他方案包括 IPSec，虽然不能满足上述全部要求，但是仍然适用于特定的环境。

2. VPN 的特点

一般情况下，一个高效、可靠的 VPN 具备了以下特点。

（1）费用低

由于使用 Internet 进行传输相对于租用专线来说，费用低廉，所以 VPN 的出现使企业通过 Internet 既安全又经济地传输内部机密信息成为可能。

（2）安全保障

虽然实现 VPN 的技术和方式很多，但这均应保证通过公用网络平台传输数据的专用性和安全性。在非面向连接的公用 IP 网络上建立一个逻辑的、点对点的连接，称之为建立一个隧道。可以利用加密技术对经过隧道传输的数据进行加密，以保证数据只被指定的发送者和接收者了解，从而保证数据的机密性和安全性。

（3）保证服务质量（QoS）

VPN 应当为企业数据提供不同等级的服务质量保证。不同的用户和业务对保证 QoS 的要求差别较大。在网络优化方面，构建 VPN 的另一重要需求是充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不到及时发送；在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策

略,可以按照优先级分配带宽资源,实现带宽管理,使得各类数据能够被合理地发送,并预防阻塞的发生。

(4) 可扩充性和灵活性

VPN 能够支持通过 Intranet 和 Extranet 的任何类型的数据流,方便增加新的节点,支持多种类型的传输媒介,可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

(5) 可管理性

在 VPN 管理方面,VPN 要求企业将其网络管理功能从局域网无缝地延伸到公用网,甚至是客户和合作伙伴。虽然可以将一些次要的网络管理任务交给服务提供商去完成,企业自己仍需要完成许多网络管理任务。所以一个完善的 VPN 管理系统是必不可少的。VPN 管理主要包括安全管理、设备管理、配置管理、访问控制列表管理和 QoS 管理等内容。

3. VPN 的连接

VPN 支持以安全的方式通过公用网络连接实现远程访问企业资源。

(1) 通过 Internet 实现远程访问

VPN 支持以安全的方式通过公用网络远程访问企业资源。与使用专线拨打长途或市话连接企业的网络访问服务器(networks access server,NAS)不同,VPN 用户首先拨通本地 ISP 的 NAS,然后 VPN 软件利用与本地 ISP 建立的连接在拨号用户和企业 VPN 服务器之间创建一个跨越 Internet 或其他公用网络的 VPN。

(2) 通过 Internet 实现网络互连

可以采用两种方式使用 VPN 连接远程局域网络:一种是使用专线连接分支机构和企业局域网;另一种是使用拨号线路连接分支机构和企业局域网。第一种方式不需要使用价格昂贵的长距离专用线路,分支机构和企业端路由器可以使用各自本地的专用线路通过本地的 ISP 连通 Internet,VPN 软件使用与本地 ISP 建立的连接在分支机构和企业端路由器之间创建一个 VPN;第二种方式是分支机构端的路由器可以通过拨号方式连接本地 ISP,VPN 软件使用与本地 ISP 建立的连接在分支机构和企业端路由器之间创建一个跨越 Internet 的 VPN。

(3) 连接企业内部网络计算机

在企业内部网络中,考虑到一些部门可能存储有重要数据,可以采用 VPN 方案来确保数据的安全性。通过使用一台 VPN 服务器既能实现与整个企业网络的连接,又可以保证保密数据的安全性。路由器虽然也能实现网络之间的互连,但是并不能对流向敏感网络的数据进行限制。而企业网络管理人员通过使用 VPN 服务器,指定只有符合特定身份要求的用户才能连接 VPN 服务器获得访问敏感信息的权利。此外,可以对所有 VPN 数据进行加密,从而确保数据的安全性。

这些 VPN 方案使用各种形式的隧道协议来实现连接。隧道协议先将网络数据包封装、加密,然后通过 Internet 安全地进行传送。在封装与加密数据包的过程中,隧道协议隐藏每个将要通过 VPN 发送的数据包的源与目的 IP 地址。

一个典型远程访问 VPN 的组成如图 7.1 所示。VPN 服务器接受来自 VPN 客户机的连接请求,VPN 客户机可以是终端计算机,也可以是路由器。隧道是数据传输通道,在其中

传输的数据必须经过封装。在 VPN 连接中，数据必须经过加密。封装数据、管理隧道的通信标准称为隧道协议。数据经过封装、加密后在隧道上传输。公用网络可以是 Internet，也可以是其他共享型网络。

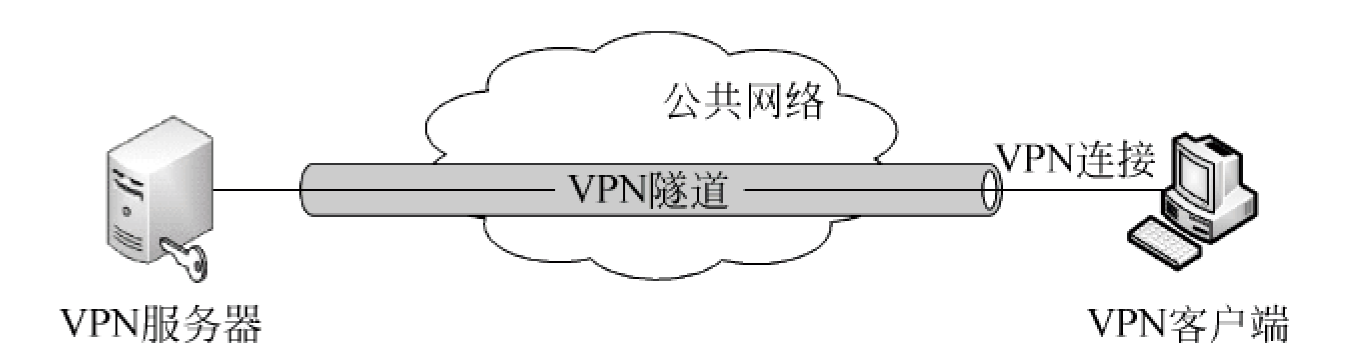


图 7.1 典型的 VPN 组成

4. VPN 关键技术

VPN 可采用多种安全技术来保证安全。这些安全技术主要有隧道(tunneling)技术、加密/解密(encryption & decryption)技术、密钥管理(key management)技术、身份认证(authentication)技术和访问控制(access control)技术等。

(1) 隧道技术

隧道技术是 VPN 的基本技术，类似于点对点连接技术。它是在公用网上建立的一条数据通道(隧道)，让数据包通过这条隧道传输。隧道是由隧道协议形成的，常用的有第 2 层和第 3 层隧道协议。第 2 层隧道协议先把各种网络协议封装到 PPP(点到点协议)中，再把整个数据包装入隧道协议中。这种双重封装方法形成的数据包依靠第 2 层协议进行传输。第 2 层隧道协议有 L2F(第 2 层转发协议)、点对点隧道协议(PPTP)和第 2 层隧道协议(L2TP)等。L2TP 协议是 IETF 标准，由 IETF 融合 PPTP 与 L2F 而形成。

第 3 层隧道协议把各种网络协议直接装入隧道协议中，形成的数据包依靠第 3 层协议进行传输。第 3 层隧道协议有 GRE、VTP 和 IPSec 等。IPSec 由一组 RFC 文档组成，它定义了一个系统来提供安全协议选择和安全算法，确定服务所使用的密钥，从而在 IP 层提供安全保障。

(2) 加密/解密技术

加密/解密技术是在 VPN 应用中将认证信息、通信数据等由明文转换为密文和由密文变为明文的相关技术，其可靠性主要取决于加密/解密的算法及强度，这部分内容在第 4 章已介绍。

(3) 密钥管理技术

密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥。现行密钥管理技术分为 SKIP 和 ISAKMP/OAKLEY 两种。SKIP 协议主要是利用 Diffie-Hellman 算法法则，在网络中传输密钥；在 Internet 安全连接和密钥管理协议(ISAKMP)中，双方都有两个密钥，分别用于公用和私用。

(4) 身份认证技术

在正式的隧道连接开始之前，VPN 要运用身份认证技术确认使用者和设备的身份，以便系统进一步实施资源访问控制或用户授权。

(5) 访问控制技术

访问控制技术决定允许什么人(用户)可访问系统，允许访问系统的何种资源以及如何

使用这些资源等。访问控制能够阻止未经允许的用户有意或无意地获取数据和授权用户的访问资源等。

7.1.2　VPN 的安全性

VPN 是一种扩展公司网络和增加网络用户功能的极好途径。许多网络管理员都未能意识到与这个扩展网络相关的许多重要的安全问题。由于允许远程用户进入公司网络的核心部分，许多限制都没有了，因此应该采取一些措施确保远程用户访问网络时不会出现安全漏洞。

1. 密码与安全认证

VPN 访问的核心问题是围绕密码进行的。在受控的网络环境下，即在已经采取必要的防范来阻止外部入侵者以及非授权用户访问网络的情况下，密码便是一种充分的验证形式。但是，密码存在着容易记忆、可破译、易被窃等问题，尤其在远程访问的情况下。因此，仅靠密码并不能为 IP VPN 提供足够的安全性。更好的一种解决方法是要求至少有一种其他形式的验证与密码验证联合使用，这就是所谓的双因素验证。例如，公司可能在要求密码验证的同时，要求有数字证书。如果不是两个级别的验证都符合要求，NAS 将拒绝验证。双因素验证极大地提高了 VPN 的安全性，但它一般要求网络中要增加额外的基础设施。证书验证需要有一个证书服务器来匹配公钥与私钥。

智能卡是一种现在越来越流行的验证形式。现在公司可能已经拥有一些不同形式的智能卡标记系统允许员工登录进入公司总部，也可使用这些智能卡标记作为一种远程验证形式。只依靠智能卡并不是非常安全的，当它们与密码或数字证书结合在一起时，便又增加一层安全保障。

生物验证是另一种验证形式。先将可用的设备插入到用户的机器中，然后公司可以根据指纹或视网膜等识别技术来进行验证。

还有一些专门的验证方法，如 RSA 有一个 SecurID 产品，它是一种硬件令牌，这个令牌与 RSA 服务器在时间上是同步的。基于这种同步，这个令牌每 60 秒生成一个新的随机数。当用户登录网络时，必须使用密码及 SecurID 令牌上的生成数进行验证。如果用户名、密码和该生成数匹配，用户便被验证通过并允许访问。

2. 扩展安全策略

如果公司网络允许远程用户访问，则要对远程用户应用安全策略。如果公司采用一些操作系统标准，那么也要求远程用户必须采用这些标准；如果公司用户必须运行最新的病毒扫描软件，那么远程用户也必须能运行这些软件。也就是说，必须要求远程用户遵循与本地用户同样的安全标准（策略）。

一些公司为了执行这一策略，为用户配发了家庭和办公室都能使用的笔记本电脑。这样即可使该电脑用户作为本地用户（内部网络用户在办公室使用）和远程用户（在家里使用）。

设备安全性只是公司安全策略的一个方面。除此之外，还要遵循如下一些安全措施。

① 当用户使用完 VPN 或短时间要离开电脑前时，必须注销 VPN。

② 密码永远也不能共享。

③ 公司的 E-mail 账户不能作为个人 E-mail 来使用。

3. 日志记录 VPN 连接

与任何远程连接一样，所有通过 NAS 进入的连接都必须有日志记录。如果出现安全问题，网络管理员可通过检查这些日志记录来确定连接初始点、时间和日期，查找事故原因。日志中除了记录网络登录外，还要尽可能多地记录会话信息。如果出现安全事故，可用的信息越多，网络管理员能跟踪并查找故障源的可能性就越大。更重要的是，如果网络中正在运行预防监控，则在日志文件中出现的任何异常，都能被很快发现；并且可能在问题发生前，阻止攻击者。

7.2 网络中 VPN 的连接

VPN 有很多端接设备，这些设备与 VPN 端接点主要有路由器、防火墙和专用 VPN 设备。

7.2.1 路由器端接 VPN

对企业网络来说，由路由器端接 VPN 并不常见。主要原因是路由器上有复杂的日志程序，并依靠外部日志资源来记录信息，再加上加密和解密 VPN 信息，因而带来较大的负担，可能造成路由器负荷很重。Cisco 已为 2600 系列路由器引进 VPN 模块。带有 VPN 模块的 2600 路由器一般用来端接 T1(1.544Mb/s 标准)，它要求至少 128MB 的随机存取内存。

路由器端接 VPN 模式要求路由器来处理好 VPN 的端接，包括加密和解密连接。

如图 7.2 所示，VPN 在边缘路由器上端接。先建立 VPN 连接到路由器，再由路由器将请求转送到 NAS。最后，NAS 验证允许访问网络的用户，并且授权用户访问网络。

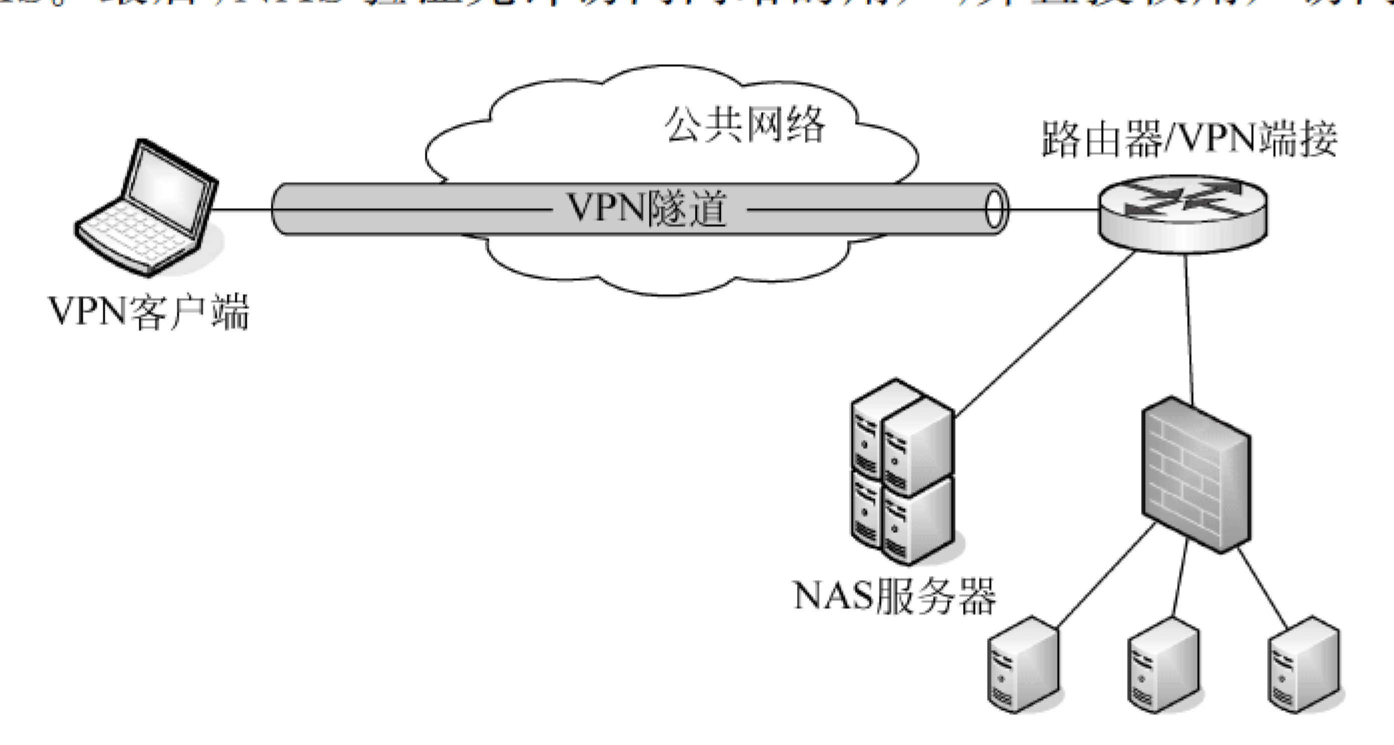


图 7.2 路由器端接 VPN

对那些不想使用 VPN 客户机程序的小型网络或家庭用户而言，路由器端接 VPN 是很方便的，但对企业网络而言，路由器端接 VPN 通常并不方便。

7.2.2　防火墙端接 VPN

目前，防火墙端接 VPN 模式是很流行的。Cisco PIX、Check Point 和 NetScreen 都有产品允许防火墙成为 VPN 端接设备。

防火墙和 VPN 的组合是很有意义的。防火墙已经记录了大多数的网络连接，再加上一些额外的 VPN 连接记录不会增加特别大的负担，且防火墙也是网络入口点，所以由防火墙端接 VPN 意味着用户能够访问网络而不必开放防火墙规则集中额外的漏洞。防火墙端接可为网络管理员提供更多的控制权。

防火墙端接 VPN 和路由器端接 VPN 的操作大致相同。用户连接防火墙，防火墙向 NAS 服务器转发验证。NAS 服务器验证用户，并且防火墙授权用户访问网络。如图 7.3 所示，从用户到公司网络的 VPN 被端接在防火墙上，防火墙收到验证请求并将它转送到处理实际验证过程的 NAS 服务器。

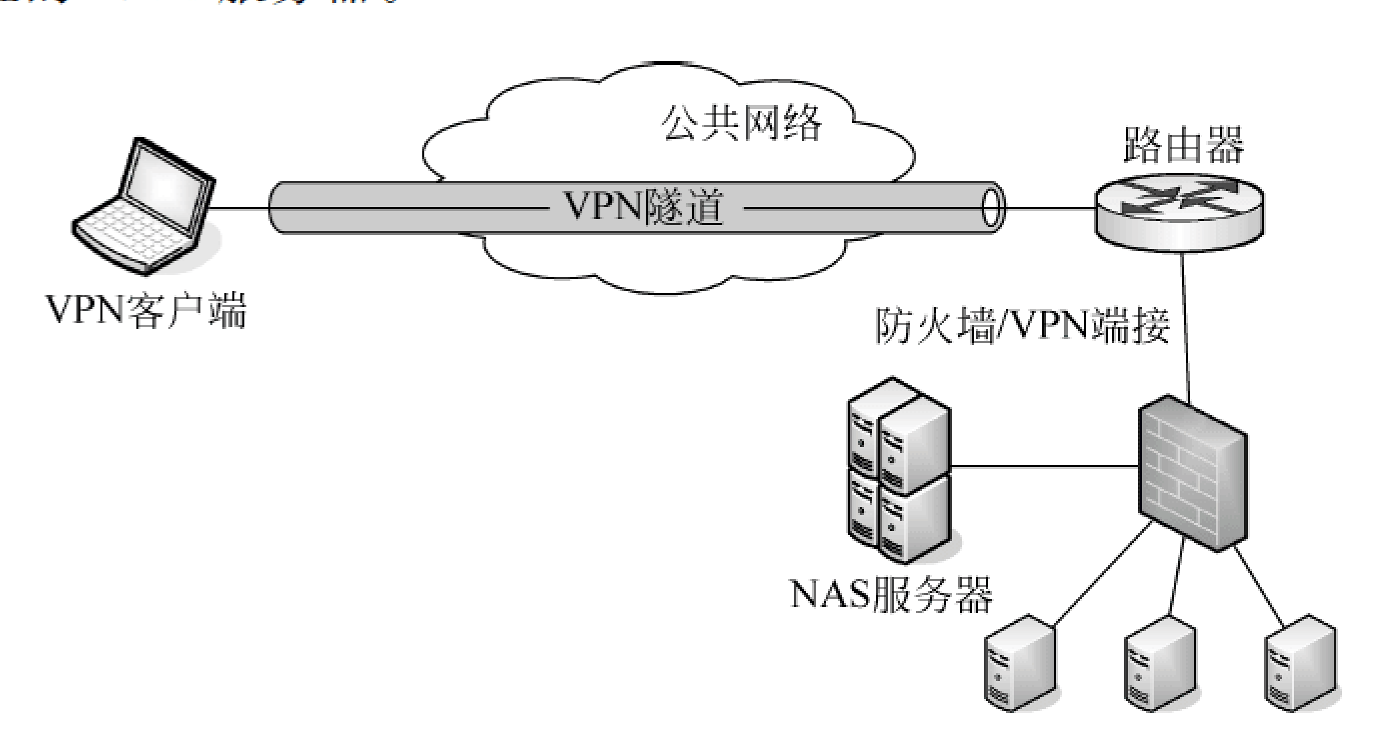


图 7.3　防火墙端接 VPN

防火墙端接 VPN 和路由器端接 VPN 连接有一个共同的缺点，就是 VPN 的加密/解密处理占用大量的系统资源。已经有负荷的防火墙，特别是带有活动 DMZ 的防火墙，很多同时运行的 VPN 隧道可能会崩溃。

防火墙端接 VPN 方案适合于企业组织，用于密切监控信息流量以确保带有 VPN 隧道的防火墙没有超负荷。

7.2.3　专用设备端接 VPN

一些公司更青睐使用专用 VPN 设备端接 VPN。Cisco、AppGate、Lucent 和 Check Point 等公司都开发出专用的 VPN 设备或在专用 VPN 上能运行的软件。

专用设备端接 VPN 的主要优点是减轻了路由器和防火墙管理 VPN 的负担。可由专用设备来处理加密和解密，即使由于过多的连接而导致它过载，也不会影响到网络的其他部分。

专用设备端接 VPN 在 VPN 处理过程中可创建另一层安全防护。它们端接在网络内部，管理员会有更大的控制权。这样就没有在路由器或防火墙上端接隧道那样的风险。在网络内部端接使网络管理员可以限定到网络某些部分的流量，这样即使 VPN 被攻破，它也可以阻止攻击者的破坏。

图 7.4 描述端接 VPN 到专用设备的过程，VPN 通过专用设备进行端接。用户可向专用设备请求验证，利用设备在网络中的位置，可限制验证后的用户到确定区域。VPN 设备也能处理验证过程，或向 NAS 转发请求。如果用户被验证成功，用户就有访问网络的权限了。

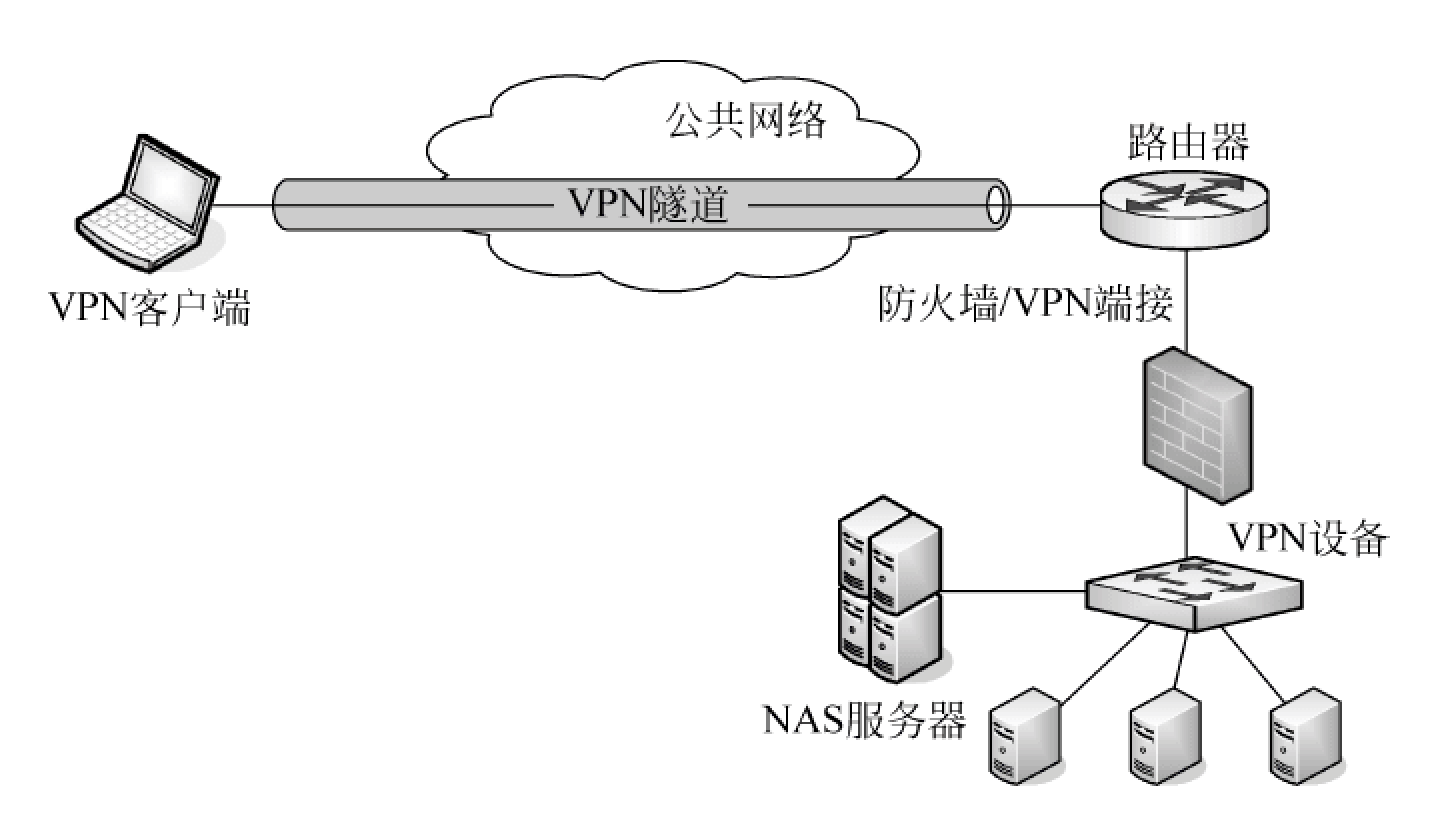


图 7.4 专用设备端接 VPN

尽管专用设备端接 VPN 有很多优点，但由于专用设备是额外的网络设备，需要对它进行管理和监控，以便软件升级和防止潜在的安全漏洞。专用 VPN 设备也存在安全漏洞，如果这些漏洞被利用，攻击者便可以访问整个网络了，因此也要关注这些漏洞的安全问题。

专用 VPN 设备也会在公司防火墙中产生额外的漏洞，因此必须打开一些端口来允许 PPTP 或 L2TP 隧道通过防火墙进入到网络。尽管这并没有引起较大的安全问题，但应该注意通过防火墙的网络流量。

7.3 VPN 的配置和应用

7.3.1 DSL 与 VPN 的连接

VPN 是通过在 Internet 或其他公用网络上建立的“隧道”来执行操作的，并可提供与专用网络相同的安全性和功能。使用 Internet，用户可从世界上大多数地方通过拨打当地的 Internet 访问电话连接到企业的办公室。如果用户的计算机和办公室具有高速 Internet 连接，那么就能以最快的速度与办公室通信。

一般情况下，企业网络及其客户都喜欢使用 DSL（数字用户线）技术连接 Internet。因此，企业在建立 VPN 前，要配置好客户端的上网环境，如将企业局域网共享一个 ADSL 连接即可连接上 Internet。这样，利用 DSL 技术实现远程管理，比任何使用模拟调制解调器的拨号连接都迅速得多，并可为企业节省很多资源。例如，运行在一条双绞线上的对称式 DSL（SDSL）可以提供与 T1 线路相同的带宽，而价格只有 T1 线路的一半。

在利用 DSL 建立 VPN 之前，用户必须确认其 DSL 服务提供商是否支持 DSL 本地环路上的多虚拟电路，是否支持多服务类型（如 CBR、VBR 和 UBR）。在可以使用多服务类型的情况下，语音虚拟电路可以被配置为 CBR 或 VBR 实时连接，这两类连接具有有限的信元

丢弃和时延,从而可保证语音质量。

DSL 和 VPN 看上去像是两个完全不相关的概念,DSL 是一种局部环技术,VPN 是关于端到端的虚拟专用网络。但事实上它们有着许多可融合之处,无论从网络的安全性、设备价格,还是从网络的速度上考虑,两者的结合都能够带来很多好处。

通过 VPN 和 DSL 的结合(基于 DSL 的 VPN—VPN over DSL),可为用户提供一个快速访问企业网络资源的途径,这要比使用调制解调器快得多。VPN 和 DSL 的融合可为用户提供一种高速的、安全的和可管理的服务。尽管目前 DSL 设备中还没有提供对 VPN 的硬件支持,但是可以在 DSL 上使用基于软件的 VPN 对企业内部网(Intranet)进行访问。

VPN over DSL 的出现并非一帆风顺,有些人认为没有必要在 DSL 上支持 VPN。他们觉得 DSL 已经比传统的拨号系统要安全得多。一个 DSL 线路是一个固定的连接,所以 IT 管理人员就已经能知道通过 DSL 进入企业网的每个呼叫是来自哪一个人或哪一个地方。另一个方面,任何拥有调制解调器和企业网远程访问拨号的人都能够拨号进入企业网,IT 管理人员却无法追查。但是,在 DSL 上支持 VPN 对于安全性所产生的好处却是毋庸置疑的。

有些 VPN 开发商已将 VPN 技术应用于其他的通信系统中,如 V-one 公司已将 VPN 技术扩展到双向寻呼机系统,ADI 公司使用 VPN 可将医疗图像安全地传送到医生家中。因此,就目前的技术而言,VPN 和 DSL 的结合是可能的。如果 DSL 的生产商在他们的硬件设备中支持 VPN 将可能使许多事情变得很简单。可以想象,在不久的将来 DSL 设备的生产商会像路由器的生产商一样在 DSL 设备中硬件支持加密体系和 IPSec 标准。

但是对于大多数的 IT 管理人员而言,他们更喜欢自己来配置 VPN over DSL,而不是等待出现支持 VPN 的 DSL 设备。对于大多数 IT 管理人员来说,使用基于软件的 VPN over DSL 还是一个相当不错的选择。另外,对于大型办公室而言,很多公司在局域网端路由器上已经使用了专门用于 VPN 的处理器。这些设备提供了 VPN 安全性问题解决方案和其他的一些功能,如流量控制管理等。从这个意义上说,公司也就没有必要在 DSL 设备上重复 VPN 的一些特性了。

7.3.2　Windows 系统中的 VPN 配置实践

本节主要介绍在 Windows 2003 环境下虚拟专用网的构建及实现 VPN 服务器和客户机的具体配置过程。VPN 连接可以通过 Internet 提供远程访问和到专用网络的路由选择连接。通过建立的 VPN 连接,使用自动安装在计算机上的点对点隧道协议 PPTP 或第 2 层隧道协议 L2TP,就可以经由 Internet 或其他网络连接到 Windows 2003 远程访问服务器(即 VPN 服务器)来安全地访问网络资源。

图 7.5 为用户直接连接到 Internet 并建立 VPN 连接的示意图。在图中可见用户主机(客户机)直接连接到 Internet,并通过 Internet 连接到远程访问服务器上。Windows 2003 系统 VPN 服务器也称为远程访问服务器。VPN 服务器必须具有一个公有 IP 地址,以便使 Internet 上的主机访问 VPN 服务器或使 VPN 客户机通过 Internet 访问 VPN 服务器。VPN 服务器一般具有双网卡,分别连接到 Internet 和内部局域网络。

1. VPN 服务器的安装

现在以基于 Windows 2003 系统为例建立 VPN 服务器。具体配置过程如下:

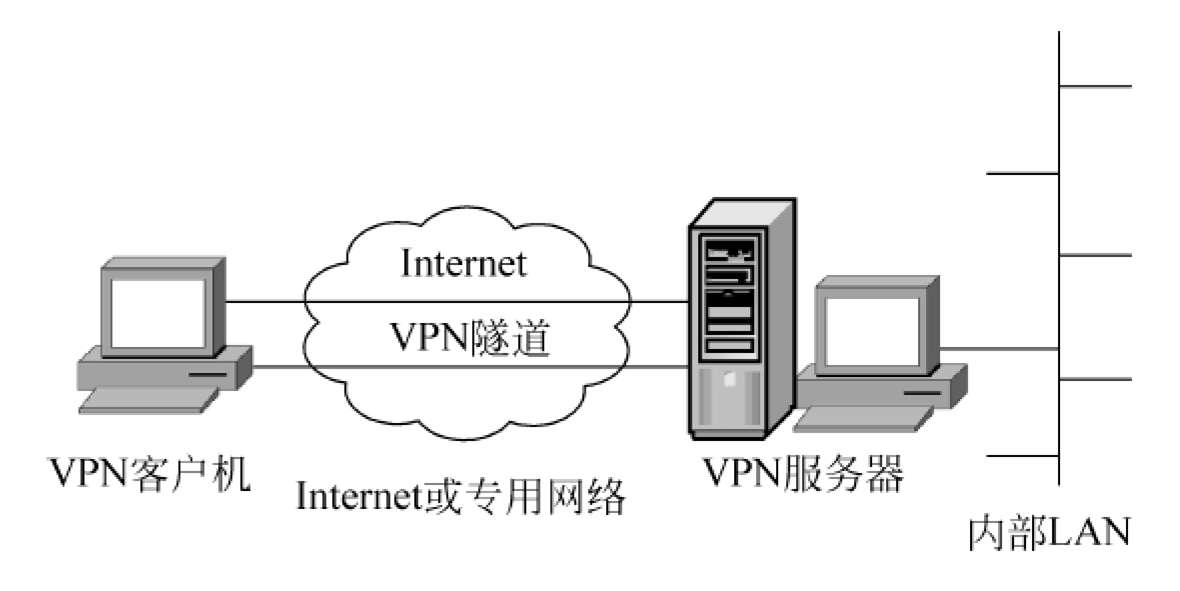


图 7.5　用户直接连接到 Internet 并建立 VPN 连接

第 1 步：选择“开始”→“程序”→“管理工具”菜单，单击“路由和远程访问”命令，在列出的本地服务器(OWNER-4T1BSHEEX)上右击，选择“配置并启用路由和远程访问”选项，如图 7.6 所示。

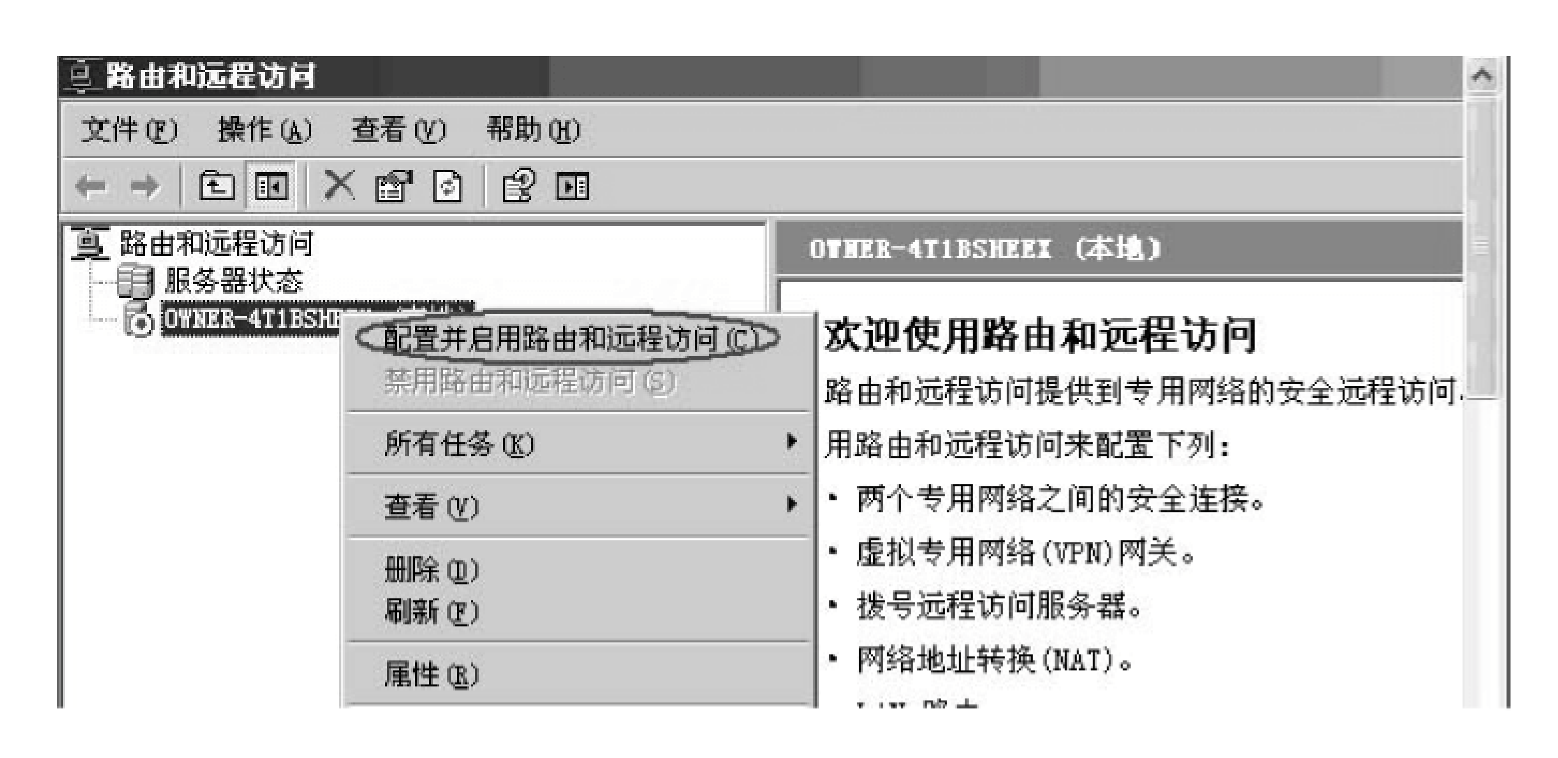


图 7.6　启用路由和远程访问

第 2 步：打开“路由和远程访问安装向导”窗口，跳过欢迎界面，单击“下一步”按钮，弹出如图 7.7 所示的窗口。在此，假设服务器是公用网络上的一般服务器，不是具有路由功能的服务器，安装有单网卡。所以这里选择“自定义配置”选项，单击“下一步”按钮。

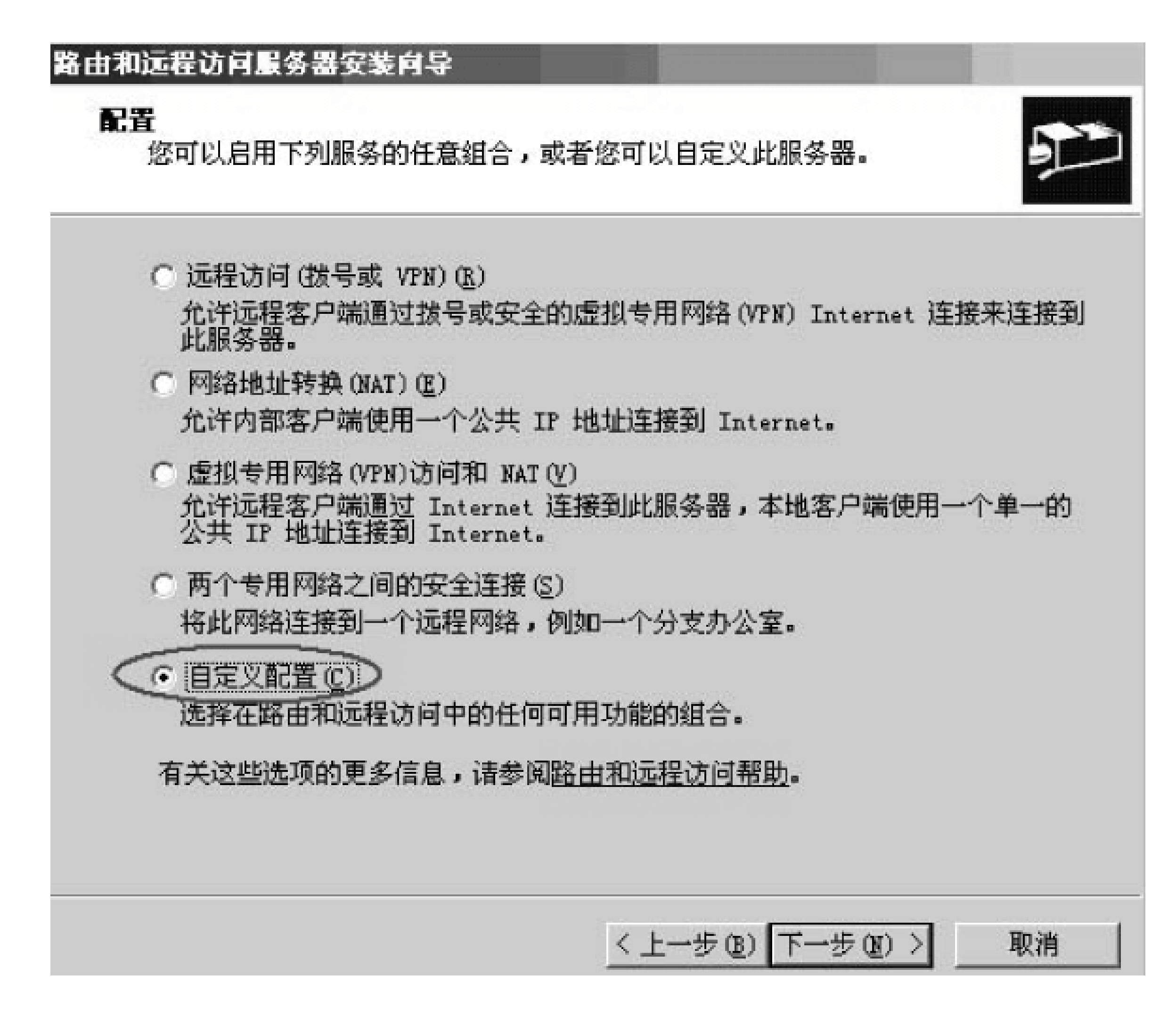


图 7.7　“路由和远程访问服务器安装向导”窗口



第 3 步：在弹出的如图 7.8 所示的窗口中选择“VPN 访问”选项，单击“下一步”按钮，配置向导完成，如图 7.9 所示。

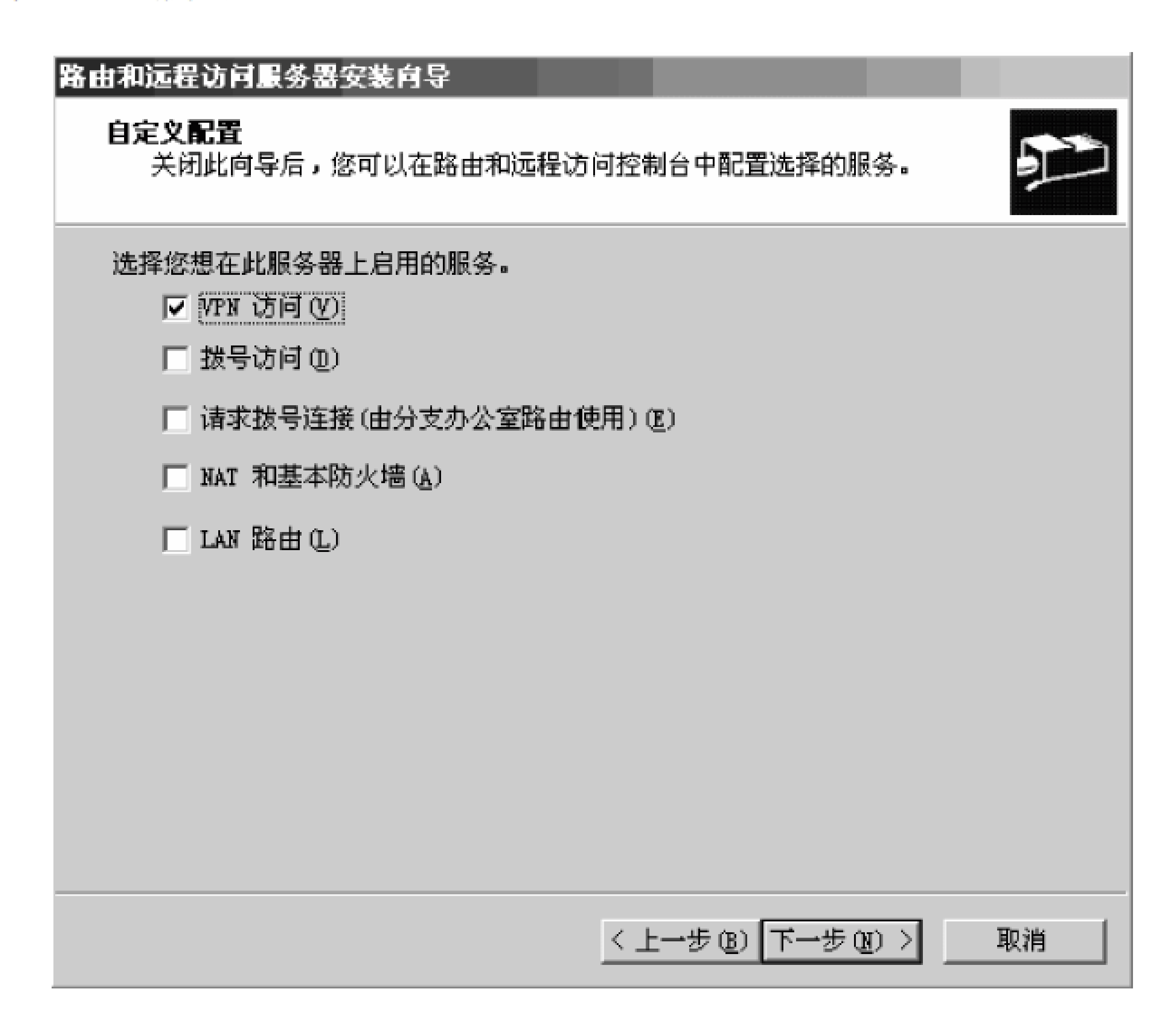


图 7.8　选择自定义配置服务



图 7.9　开始路由和远程访问服务

第 4 步：在图 7.9 中的提示“路由和远程访问服务现在已被安装。要开始服务吗?”下单击“是”按钮，VPN 开始服务。

2. VPN 服务器的配置

启动 VPN 服务后，出现如图 7.10 所示“路由和远程访问”界面，可在此界面下进行 VPN 服务器的配置。



图 7.10 进入路由和远程访问界面

第 1 步：在图 7.10 中右击服务器(OWNER-4T1BSHEEX)，选择"属性"菜单，弹出如图 7.11 所示的"OWNER-4T1BSHEEX(本地)属性"窗口。选择启用此计算机作为"路由器"或"远程访问服务器"复选项。

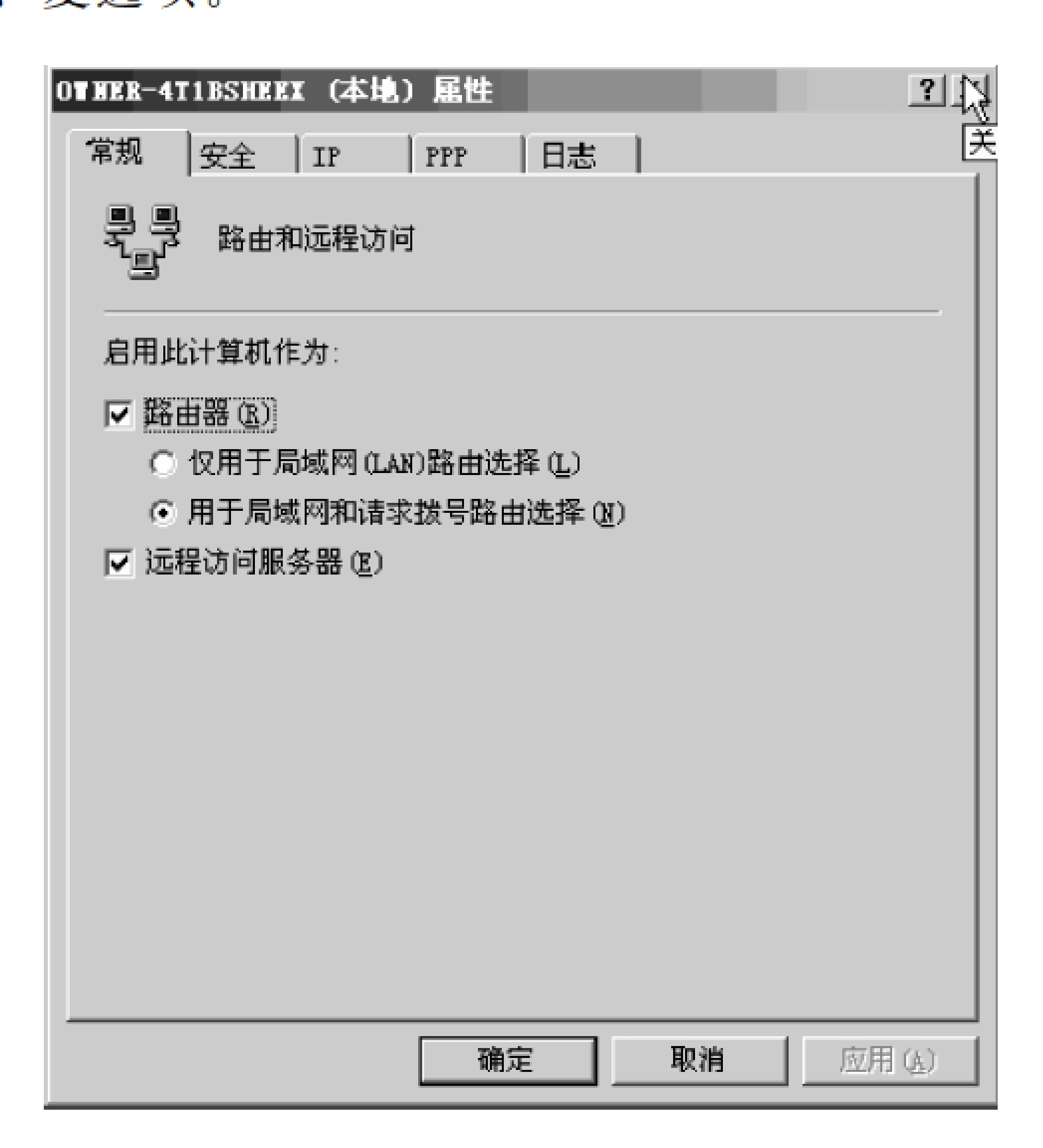


图 7.11 VPN 服务器属性窗口

第 2 步：在该"属性"窗口中选择"IP"选项卡，如图 7.12 所示，勾选"启用 IP 路由"和"允许基于 IP 的远程访问和请求拨号连接"选项。在"IP 地址指派"中选择"静态地址池"，设置 IP 地址范围。单击"添加"按钮，在弹出的"新建地址范围"窗口中输入起始 IP 地址和结束 IP 地址，这样就设置了一个 IP 地址范围。

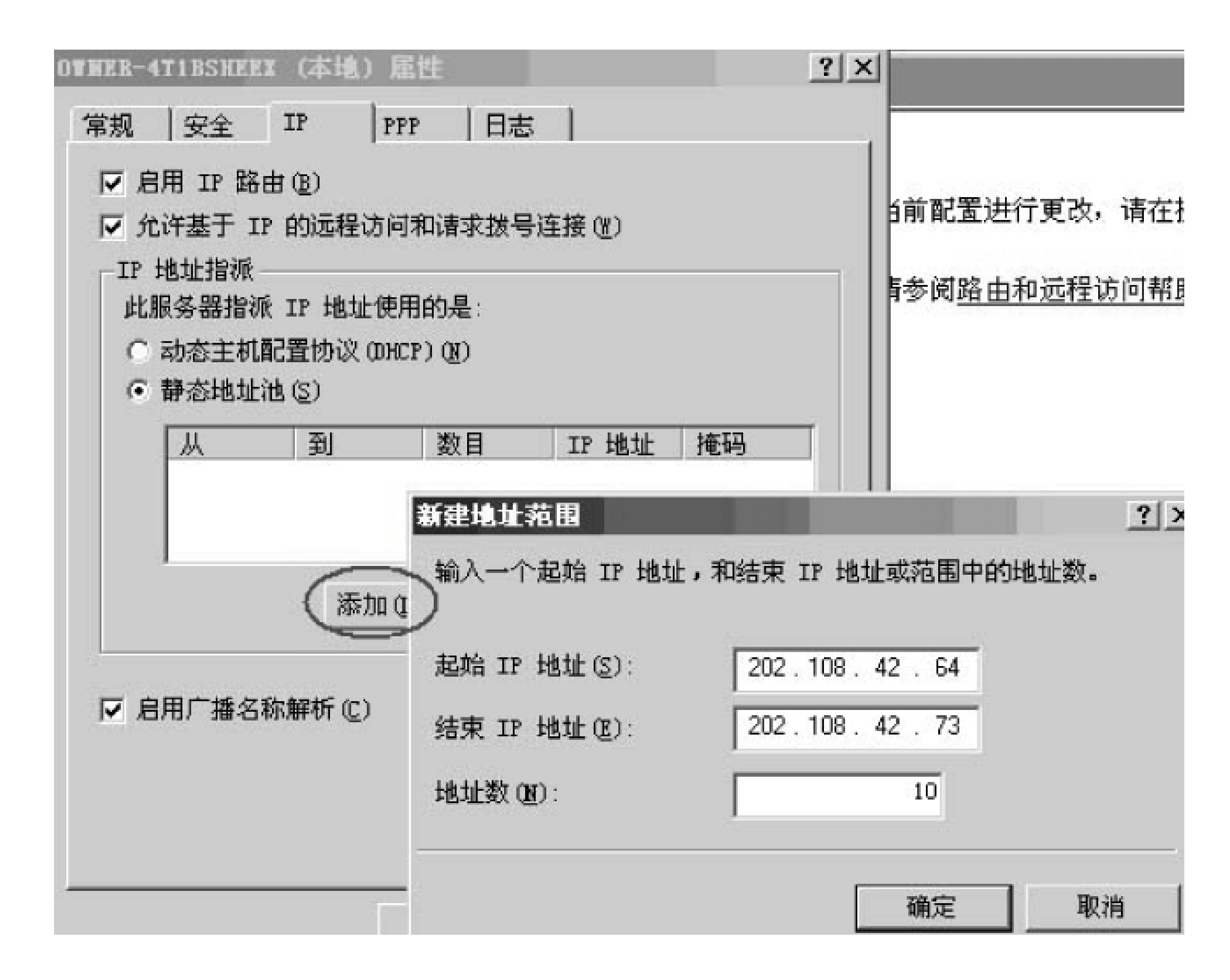


图 7.12　IP 地址范围设置

第 3 步：单击“确定”按钮，弹出如图 7.13 所示窗口，再单击“确定”按钮，即完成 IP 地址设置。

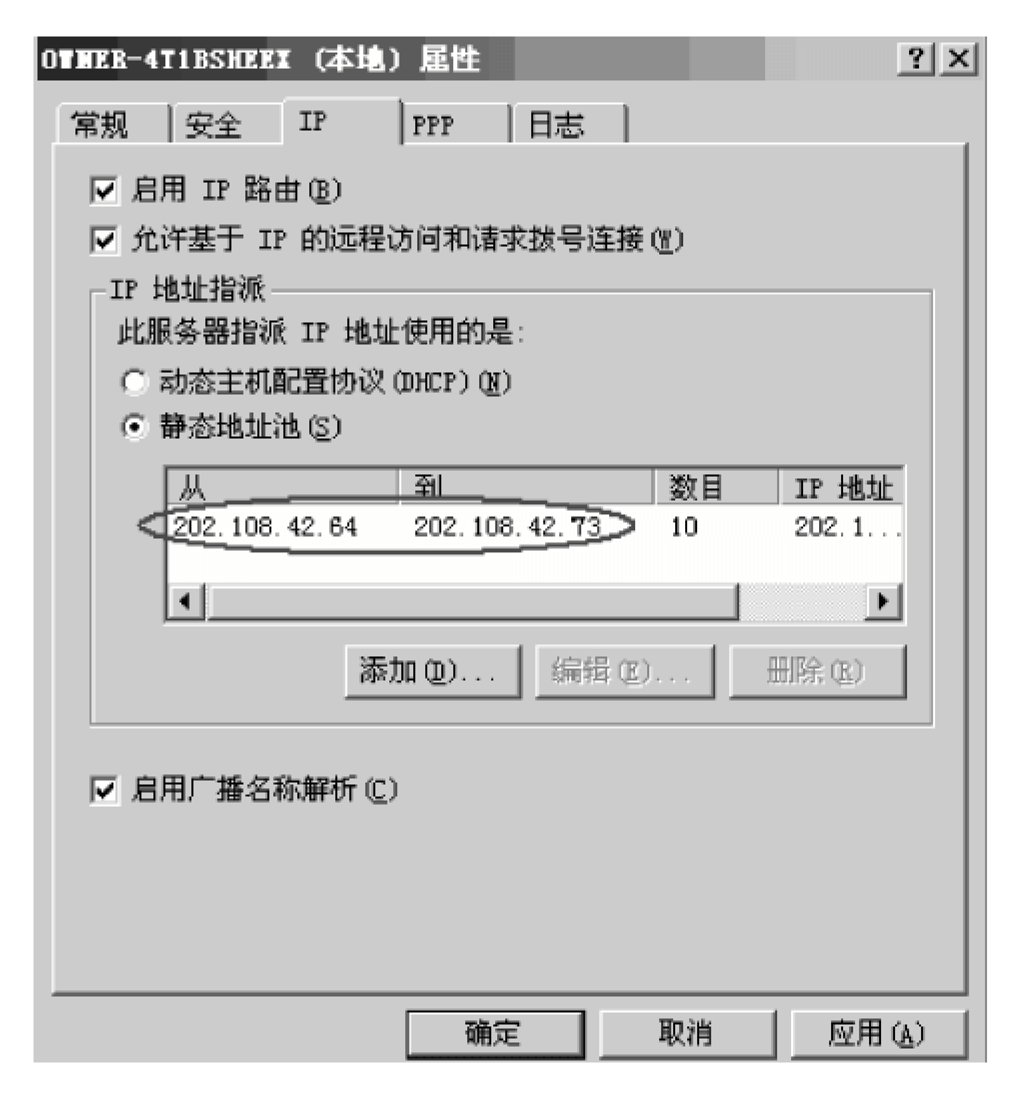


图 7.13　完成 IP 地址设置

至此，完成了 VPN 服务器部分的配置。

这里的 IP 地址范围就是 VPN 局域网内部的虚拟 IP 地址范围，每个拨入到 VPN 服务器的用户都会分配到该范围内的一个 IP 地址。用户可在虚拟局域网中用各自分得的 IP 地址相互访问。本例中设置的 IP 地址范围为 202.108.42.64～202.108.42.73，共 10 个 IP 地址。默认的 VPN 服务器占用第一个 IP。所以，202.108.42.64 实际上就是这个 VPN 服务器在虚拟局域网的 IP 地址。

3. 添加 VPN 用户并赋予用户拨入权限

每个要拨入 VPN 服务器的客户端都需要有一个账号。要给每个需要拨入到 VPN 的客户端设置一个用户,并为这个用户制定一个固定的内部虚拟 IP 地址,以便客户端之间相互访问。默认情况下所有用户均被拒绝拨入到 VPN 服务器上,因此 VPN 服务器的配置过程结束后需要添加用户,并为相应用户赋予拨入权限。

在 VPN 服务器上,利用"管理工具"中的"计算机管理"里添加用户,这里以添加一个"ysliu"用户为例,过程如下:

第 1 步:选择"开始"→"程序"→"管理工具"菜单,单击"计算机管理"命令,打开其控制台。

第 2 步:选择"系统工具"→"本地用户和组"菜单,单击"用户"命令,则可以看到所有的本地用户,如图 7.14 所示。



图 7.14 本地当前用户显示

第 3 步:右击"用户"命令,选择"新用户"来新建一个用户。用户名可以取为 ysliu,并选择和确认密码(从安全角度考虑,用户名和密码要设置得复杂些),如图 7.15 所示,并将"用户下次登录时必须更改密码"前的选项去掉。单击"创建"按钮,即创建完一个用户。如果还想创建其他用户,重复以上过程即可。

第 4 步:创建好 ysliu 用户后,在"计算机管理"控制台的用户栏即可看到该用户,如图 7.16 所示。

第 5 步:右击用户名 ysliu,选择"属性"菜单,弹出如图 7.17 所示新用户属性窗口。在"ysliu 属性"窗口单击"确定"按钮,弹出如图 7.18 所示窗口。

第 6 步:打开图 7.18 中的"拨入"选项卡,在"选择访问权限(拨入或 VPN)"选项组下选中"允许访问"(允许这个用户通过 VPN 拨入服务器)。单击"分配静态 IP 地址"选项,并设置一个

新用户
用户名(U): ysliu
全名(F): ysliu
描述(D): 一般用户
密码(P): ******
确认密码(C): ******
用户下次登录时须更改密码(M)
用户不能更改密码(S)
密码永不过期(W)
账户已停用(B)
创建(E) 关闭(O)

图 7.15 新建用户信息输入



图 7.16　显示本地新用户

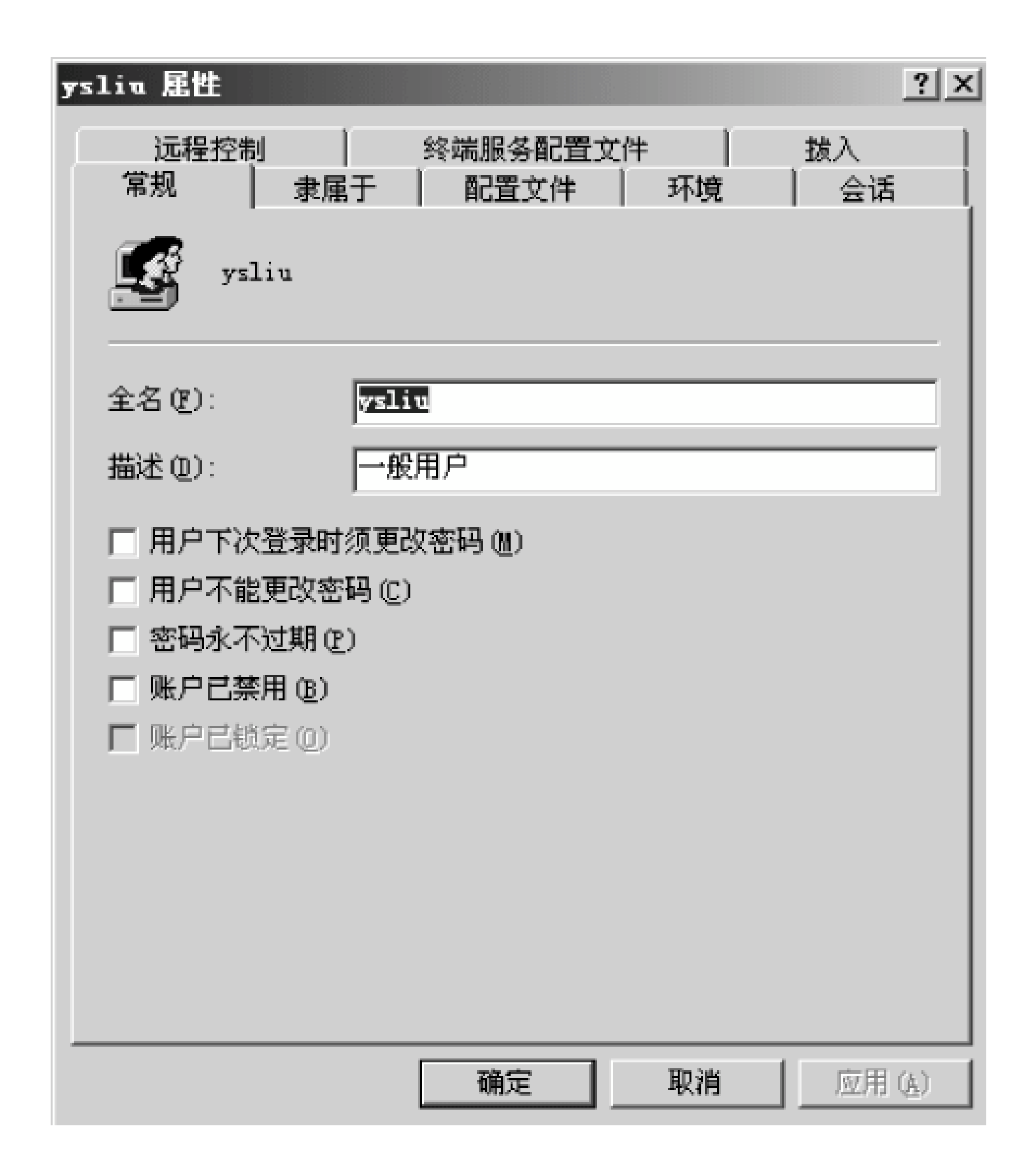


图 7.17　新用户属性(1)

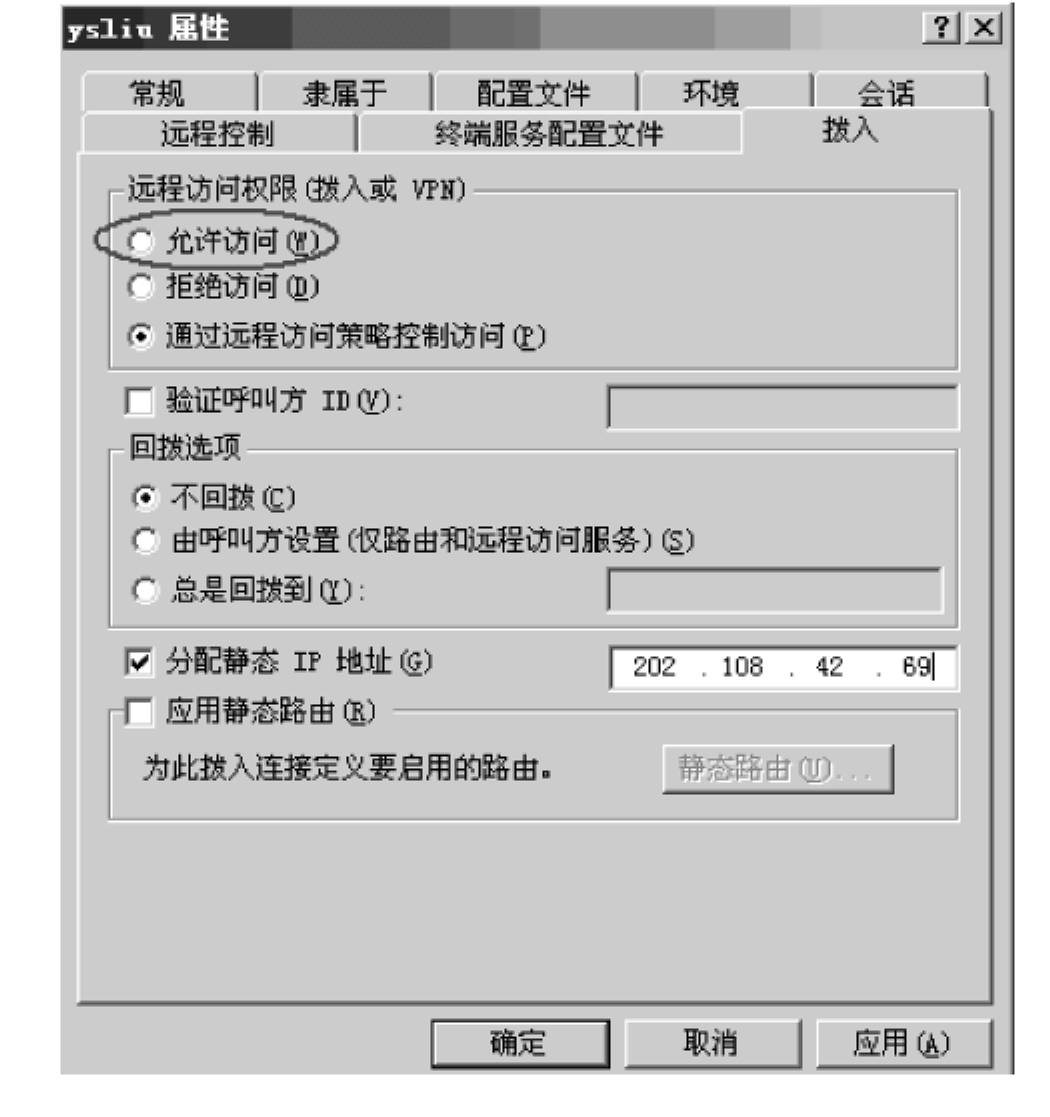


图 7.18　新用户属性(2)

VPN 服务器中静态 IP 池范围内的一个 IP 地址作为该用户的 IP,这里设为 202.108.42.69。

第 7 步:单击“确定”按钮,返回“计算机管理”控制台。

至此,即结束了创建新用户和赋予新用户拨入权限的工作。

如果有多个客户端机器要接入 VPN,则可按上述步骤为每个客户端都新建一个用户,并设定一个虚拟 IP 地址,各个客户端都使用分配给自己的用户拨号 VPN,这样各客户端每次拨入 VPN 后都会得到相同的 IP。如果用户没设置为“分配静态 IP 地址”,客户端每次拨入到 VPN,VPN 服务器会随机给这个客户端分配一个范围内的 IP。

4. VPN 客户端的设置与连接

VPN 客户端可以基于 Windows XP 系统,也可以基于 Windows 2003 系统,在此以 Windows XP 系统为例(该客户端计算机可通过 ADSL 技术拨号上网)进行设置。

第 1 步：在客户机上依次选择"开始"→"设置"→"控制面板"菜单，打开"网络连接"对话框，单击"创建一个新的连接"选项，在"新建连接向导"中选择"连接到我的工作场所的网络"选项，如图 7.19 所示。

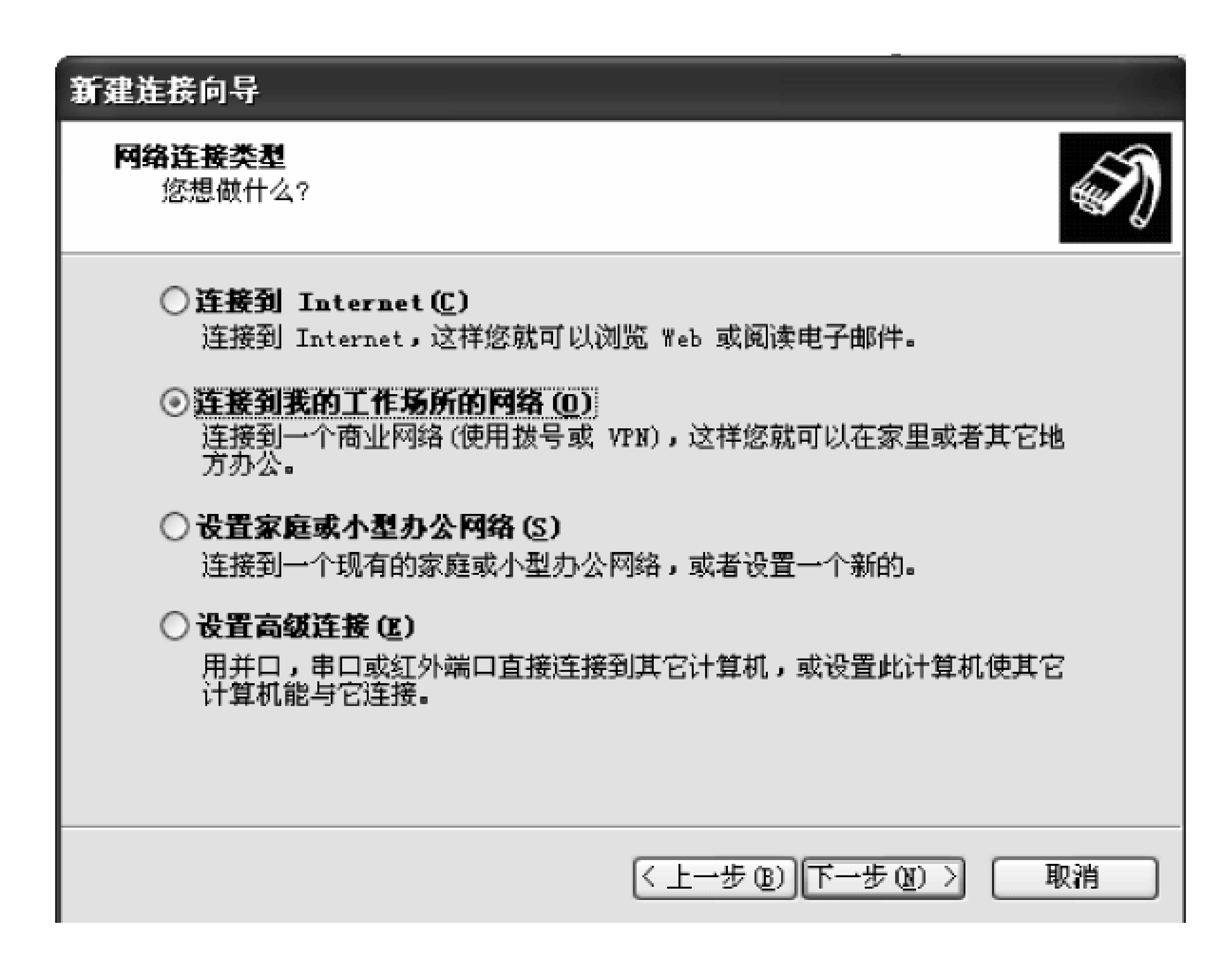


图 7.19　新建连接向导之网络连接类型

第 2 步：单击"下一步"按钮后弹出如图 7.20 所示窗口。在"创建下列连接"的单选栏中选中"虚拟专用网络连接"选项。



图 7.20　新建连接向导之网络连接

第 3 步：单击"下一步"按钮，在弹出的如图 7.21 所示的窗口"连接名"对话框中为连接输入一个公司名，如 ABC；单击"下一步"按钮后，在弹出的如图 7.22 所示窗口中输入准备连接的 VPN 服务器的 IP 地址或域名，如 www.163.com。

第 4 步：单击"下一步"按钮后，完成新建连接。

这样，在"控制面板"的"网络连接"中的"虚拟专用网络"下面，就可以看到刚才新建的 ABC 连接，如图 7.23 所示。



图 7.21　新建连接向导之连接公司名称



图 7.22　新建连接向导之服务器域名



图 7.23　新建的 VPN 连接

第 5 步：在 ABC 连接上右击，再单击“属性”按钮，在弹出的窗口中单击“网络”选项卡，然后选中“Internet 协议(TCP/IP)”选项，如图 7.24 所示。

第 6 步：单击图 7.24 中的“属性”按钮，在弹出的窗口中再单击“高级”按钮，把“在远程网络上使用默认网关”前面的钩去掉，如图 7.25 所示。



图 7.24 新建连接的属性



图 7.25 高级 TCP/IP 设置

注意：如果不取消这个勾选，客户端拨入到 VPN 后，将使用远程的网络作为默认网关，致使客户端只能连通虚拟局域网而连不上 Internet。

第 7 步：现在可以开始拨号进入 VPN 了。双击图 7.23 中的 ABC 连接，弹出如图 7.26 所示窗口。

第 8 步：在图 7.26 中单击“属性”按钮，弹出如图 7.27 所示“宽带连接 属性”窗口。



图 7.26 拨号连接属性



图 7.27 拨号连接的安全属性

第 9 步：在图 7.27 中打开“安全”选项卡，单击“高级”选项，再单击“设置”按钮，弹出如图 7.28 所示的“高级安全设置”窗口。按图示对数据加密允许使用的协议进行相应的选择后，单击“确定”按钮。



图 7.28　拨号连接的高级安全设置

第 10 步：进行高级安全设置后，在图 7.26 对话框的用户名和密码栏分别输入分配给该客户端的用户名和密码。然后单击“连接”按钮，片刻后即可看到此次拨号连接完成的显示，表示已经拨通入网了。

拨通后在任务栏的右下角会出现一个网络连接的图标，表示已经拨入到 VPN 服务器。

如果希望每次拨号时均不用再输入用户名和密码，则可在图 7.26 中勾选“为下面用户保存用户名和密码”选项，并勾选“只用我”或“任何使用此计算机的人”选项。为了安全起见，建议每次拨号入网时要输入自己的用户名和密码。

以上是通过 Windows 2003 提供的“路由和远程访问”功能配置实现 VPN 服务器，并通过建立 VPN 客户端实现 VPN 连接，使位于异地的主机能够通过 VPN 连接的方式组建成新的 VPN 网络，使其能够访问到没有分配公有 IP 地址的内部网络主机并具有良好的保密性。

如果想查看 VPN 客户端与服务器的连接，可在客户机上依次单击“开始”→“程序”→“附件”→“命令提示符”菜单，在命令提示符窗口输入 ipconfig 并按回车键，这时可以看到本地连接的 IP 地址和虚拟专用连接的 IP 地址。同样，在 VPN 服务器端也可以看到已经建立起来的 VPN 连接情况。

另外，VPN 服务器的远程访问策略可以灵活地对远程访问进行配置，建议网络管理员使用该项功能。配置远程访问策略可在图 7.10 中的“远程访问策略”下进行(右击“远程访问策略”选项，选择“新建远程访问策略”，在出现的“新建远程访问策略向导”中跳过欢迎界面，依次在“策略配置方法”、“访问方法”、“用户或组访问”等对话框中填入相应信息即可)。

习题和思考题

一、问答题

1. 什么是虚拟专用网(VPN)? VPN 采用了哪些安全措施?

2. 简述 VPN 的功能和特点。

二、填空题

1. VPN 采用了(　　)、(　　)、(　　)和完整性等安全措施。

2. VPN 采用的安全技术主要有(　　)技术、(　　)技术、(　　)技术、(　　)技术和访问控制等。

3. VPN 的主要端接点有(　　)、(　　)和专用 VPN 设备。

三、单项选择题

1. 以下(　　)项是 VPN 的功能。

A. 数据加密　　B. 用户认证　　C. 多协议支持　　D. A、B、C 都对

2. 以下(　　)项可能不是 VPN 的特点。

A. 低费用　　B. 高安全性　　C. 高速率　　D. 高质量

四、实验题

VPN 实验:参考本教材或相关手册,进行 Windows 2003 环境下 VPN 服务器的安装与配置。

第8章 无线网络的安全与应用实践

自从意大利人马可尼在1896年申请了第一个无线电报专利以来,无线技术已经改变了人们接收信息的方式。从最早的收音机到现在的手机、无线网络设备,无线通信得到了长足发展,也催生了一系列的产品和服务。

无线技术与网络技术的融合提供了即时通信、永久在线的可能性,其发展前景似乎是无限的。但作为一种新型技术,新的标准和应用发展很快,安全问题却没有得到足够重视。无线通信中信息是利用无形介质传输的,因此更容易被截收,信息安全问题更加突出。C. I. A(信息安全体系的三大目标:保密性(Confidential)、完整性(Integrity)和可用性(Availability),简称为C. I. A)的要求同样适合于无线网络。随着无线技术的发展,其安全技术也得到发展,无线网络安全标准WTLSP和802.1x等正在逐步得到完善。

8.1 无线广域网安全

8.1.1 无线广域网技术

无线网络有无线局域网(WLAN)和无线广域网(WWAN)两种类型。WWAN技术的主要用途是连接Internet和将分散在城市各处的用户点连接起来。可使常用的笔记本电脑或其他设备在蜂窝网络覆盖范围内的任何地方连接到Internet。

1. MMDS技术

多信道多点分配业务(multichannel multipoint distribution services,MMDS)始于20世纪80年代,开始时服务于无线电视用户。MMDS技术发展初期,FCC(美国联邦通信委员会)分配了4组8个频道,这意味着无线电缆公司只能向其用户发送4个频道的节目。因为在电视系统中,频道数越多越好,基于MMDS技术的电缆公司向FCC请示分配更多的频道,因而发展成后来的频率分发技术。

MMDS工作于2.5~2.7GHz频段。接收器通常是全方向的,允许从各个方向进行连接。由于MMDS工作于一个相对低的频率,它对大气条件有一定的抵抗力,而且一个天线就可以服务很大的范围。

由于其部署相对便宜,很多公司还是支持MMDS应用于无线系统。一个安装足够高的单个天线,可以服务很大的区域。ISP将连接接入Internet之前可以通过多个天线路由

连接。这可使 ISP 通过设置连接多个天线形成骨干连接的方式以节省带宽投资。它还允许 ISP 为其客户设置冗余连接。可以创建一个无线天线环来为某一区域提供服务，提供数据传送过程中的容错能力，甚至可以为 ISP 的用户提供多点连接。

2. LMDS 技术

本地多点分配业务(local multipoint distribution services，LMDS)也是一种固定式无线技术，但它的支持技术与蜂窝式技术类似。LMDS 工作于 28～31GHz 频段，其服务范围比 MMDS 小，仅支持方圆 5 英里的通信，且只有大约 2.5 英里的全带宽通信能力。LMDS 比 MMDS 更易受天气和其他干扰的影响。

LMDS 的优势在于它部署的单个访问天线的价格较低，且使用频率较高，可允许供应商为每个客户提供更大的带宽。LMDS 供应商可提供 10Mb/s 的下载速率和 2Mb/s 的上传速率。由于 LMDS 服务范围的限制及其所需的严格线路，LMDS 适合在城市或商业区部署。

3. 扩频技术

扩展频谱技术(spread spectrum technology，SST，简称扩频技术)是一种宽带无线电频率(radio frequency，RF)技术。在发送端，SST 将窄频固定无线信号转化为宽频信号输出；在接收端，无线数据终端系统(WMTS)接收宽频信号，并将其转变为窄频信号并对信息进行重组。

扩频技术采用一种比窄带传输消耗更多带宽的传输模式，但却能够产生更强、更能被其他设备接收到的信号。因此，扩频技术牺牲了带宽，却带来安全性、信息完整性和传输可靠性方面的优势。扩频技术有跳频扩频(FHSS)、直接序列扩频(DSSS)和码分多址(CDMA)三种类型。

CDMA 主要应用于移动电话业务。CDMA 以与 DSSS 和 FHSS 相同的方式转换数据，但与 FHSS 和 DSSS 相比，它通过更窄的波段来扩散信号。

4. 无线应用协议(WAP)

1997 年，爱立信、摩托罗拉、诺基亚等公司公布了无线应用协议(wireless application protocol，WAP)。WAP 是作为一组技术开发的，只是它更适应小屏幕、资源有限的手持设备的应用。WAP 的最新版本允许用户通过电话传输动画和声音等多媒体文件。它包括一个工具包，使得新的应用(如 XHTML)能够更快地被开发出来。

WAP 是一种无线应用通信协议，是一种向移动终端提供 Internet 内容和先进增值服务的、全球统一的开放式协议标准，是简化了的无线 Internet 协议。这项技术让使用者可以用手机之类的无线装置上网，透过小型屏幕访问各个网站。而这些网站以前必须以 WML 编写，但是在手机功能越来越强大的今天，这类网站不再只能用 WML 语言编写，还可以使用 XHTML 语言，编写出来的页面功能更丰富。它不依赖某种网络而存在，今天的 WAP 服务在 3G 普及后仍然可能继续存在，不过传输速率更快，协议标准也会随之升级。

WAP 的目标就是通过 WAP 技术将 Internet 的大量信息及各种各样的业务引入到移动电话、PALM 等无线终端之中。无论用户在何时何地，只要需要信息，就可以打开自己的

WAP手机上网，享受无穷无尽的网上信息或网上资源，如综合新闻、天气预报、股市动态、商业报道、当前汇率等。WAP的电子商务、网上银行也将逐一实现。

8.1.2　无线设备与数据安全

1. 无线频率安全

由于无线传输是通过无线电波进行的，这使任何人不必经过物理连接到网络的任何部分即可监控传输过程。拥有无线网卡和一些无线网络系统基本知识的攻击者即可监控所有通过网络的通信。

大多数形式的固定无线Internet访问通过RF频谱进行通信。RF频谱实际是一个宽范围的微波频率，范围从500kHz～300GHz。常见的使用RF频谱的设备有移动电话、无绳电话、电视机、AM和FM收音机、微波炉等。

RF频谱内频率的使用，在美国由FCC授权许可，而世界其他地方由国际电信联盟(ITU)授权许可。这种差异会导致美国的设备与世界其他国家的同类设备运行在不同的频率上。

并不是RF频谱内所有的频率都要经过许可，还有一些频率范围为自由频段，最常用的是工业、科学和医学(industrial、scientific、medical，ISM)界所用的频段。ISM频率通常是固定式无线Internet访问设备所最常用的频率。

最常用的两种固定式无线Internet访问技术为MMDS和LMDS。

2. 物理位置安全

无线网络重要设备的物理位置对于固定式无线通信环境来说是非常重要的，其主要原因是信息的可到达性和设备的安全性。

信息可到达性是固定式无线网络用户最关心的事，尤其是应用LMDS技术的用户。如果天线没有ISP的WMTS清晰视线，连接就会被认为是无用的。多数情况下，需要访问WMTS的视线意味着要求天线必须安装在无线网络设备所在的建筑物顶部或建筑物外的高塔(杆子)上。这样可使信息有最大化的可到达性。另外，提高无线网络性能的一个途径是通过使用更好的电缆，这可有助于降低信号衰减。

为了保证设备的安全性，用户可考虑将一些重要设备(如无线调制解调器、路由设备)固定在安全的箱柜里。调制解调器上的默认密码应该改变，而且还要限制能访问它的用户数量。一些公司希望将调制解调器放在天线附近，通常是放在屋顶，作为保持信号强度的方法。在这种情况下可将调制解调器加锁封装，以防止自然环境的破坏和潜在的攻击者。如果条件允许，可建筑一道篱笆围起调制解调器和天线，确保这些重要物理设备的安全。

3. 无线数据加密

固定式无线传输通过使用扩频技术来保证其安全。由于无线连接通过特定频段传输(如FM信号)，所以某个拥有天线和类似网络设备的攻击者会很容易地嗅探到传输信息。

保护传送数据安全的最好办法是对数据进行加密。无线制造商开发了一种基于电缆的安全标准——缆上数据业务接口规范(DOCSIS＋)系统。使用DOCSIS＋系统，ISP可以对

用户调制解调器和IWMTS(无线消息测试平台)之间的数据流进行强制加密。DOCSIS+系统支持多种类型的密钥体制(如x.509数字认证、RSA公钥加密算法和TDES加密)。WMTS制定的加密策略要求终端用户调制解调器必须遵守,否则WMTS不接收数据。这样既可防止攻击者查看数据,又可防止未授权用户用WMTS获得对ISP的未授权访问。

8.1.3 无线蜂窝网络技术

1. 无线传输技术

第一代无线传输技术(1G)是基于模拟信号的,其传输速率为9.6Kb/s或更低。第二代无线传输技术(2G)是基于数字信号的,其标准有美国的TDMA和CDMA、日本的PDC及欧洲的GSM。2G能够提供更高的传输速率和更好的安全性,其传输速率为9.6~14.4Kb/s。第三代无线传输技术(3G),如UMTS和CDMA 2000,其传输速率可达到14.4Kb/s~2Mb/s。在2G与3G之间还存在着第2.5代(2.5G),它属于第二代的功能提升及向第三代的过渡。第四代无线传输技术(4G)着眼于无线异步传输模式(WATM)的研究上,它能够提供10Mb/s~150Mb/s的高质量、低差错率的服务,也就是真正的高速无线数据网络。

2. 时分多址

时分多址(time division multiple access,TDMA)技术是美国电信产业协会(TIA)于1992年制定的数字标准,属于第二代无线传输技术。TDMA将分配给它的频宽划分成一系列的信道,每个信道划分为多个时段,信道中的每个会话被分配到这些时段里。许多电信运营商将其加入到以前的语音网络中,以提高它的安全性和功能。

3. 全球移动通信系统

全球移动通信系统(global system for mobile communications,GSM)是世界上主要的蜂窝技术之一。GSM是基于窄带TDMA制式,允许在一个射频同时进行8组通话。GSM在20世纪80年代兴起于欧洲,1991年投入使用,到1997年底,已经在100多个国家运营,成为欧洲和亚洲实际上的标准,属于2G技术。

随着GSM移动通信网络用户数量的迅速增长,为了满足GSM网络容量增长的需求,GSM在原有的900频段的基础上,又引入1800频段。采用GSM900/1800双频段操作,极大地缓解了GSM900的容量压力。采用GSM900/1800双频段操作,能经济有效地解决网络容量需求的问题。

4. 码分多址

码分多址(code division multiple Access,CDMA)技术于1993年被电信产业协会(TIA)采用,其主要特点是高质量、小蜂窝半径、特殊编码方式和扩频技术。它是在扩频通信技术上发展起来的一种崭新而成熟的无线通信技术。CDMA技术的原理是基于扩频技术,即将需要传送的具有一定带宽的数据信号,用一个远大于此信号带宽的高速伪随机码进行调制,使原数据信号的带宽被扩展,再经载波调制并发送出去。接收端使用完全相同的伪

随机码，与接收的带宽信号做相关处理，把宽带信号转换成原来的窄带信号（解扩），以实现数据通信。

5. 2.5G 技术

第 2.5 代无线通信技术能够提供更高的带宽和更多的服务内容，如 HSCSD、GPRS 和 EDGE 技术。它们可使网络运营商在投资到昂贵的 3G 技术之前就能给用户提供增强的服务。

高速线路交换数据（high speed circuit switched data，HSCSD）是一个基于 GSM 的线路交换协议。它的速率能够达到 38.4Kb/s，这是因为它能够使用 4 条信道同时提供 GSM 服务，是过渡到 GPRS 的中间技术。

通用分组无线业务（general packet radio service，GPRS）是基于 GSM 的分组交换技术，其速率能够达到 144Kb/s。GPRS 设备一直和网络连接，这意味着它能够提供即时通信功能。当有数据传输时，才需要占用网络带宽。

增强型数据速率 GSM 演进技术（enhanced data rate for GSM evolution，EDGE）是一种从 GSM 到 3G 的过渡技术，它主要是在 GSM 系统中采用了一种新的调制方法，即最先进的多时隙操作和 8PSK 调制技术。EDGE 能够提供 384Kb/s 的速率，就能够支持无线多媒体应用。

6. 3G 技术

第三代移动通信（3G）技术能够提供更高的速率。它的技术框架由 ITU 作为 IMT-2000 项目的一部分制定。3G 是第一个将宽带数据通信和语音通信放到同等位置的无线蜂窝技术。蓝牙技术规范也支持 3G 技术，将各种服务扩展到掌上电脑和 PDA（personal digital assistant）上。

国际移动电话标准 2000（IMT-2000）项目是为促进 3G 技术开发者之间的合作而设立的。通用移动通信系统（universal mobile telecommunications system，UMTS）是欧洲电信标准协会（ETSI）提出的项目。它是 IMT-2000 标准在欧洲的第一个应用。UMTS 是下一代全球蜂窝系统，已投入使用。通过同时使用在 2GHz 频段的 TDMA 和 WCDMA，UMTS 将达到 2Mb/s 的带宽。WCDMA（宽带 CDMA）和 TD-SCDMA（时分同步码分多址）技术同属 3G 技术。WCDMA 是一种基于 GSM MAP 核心网、利用码分多址复用方法实现的宽带扩频的 3G 系统，支持 WCDMA 的厂商有爱立信、诺基亚和一些日本厂商。TD-SCDMA 是由中国提出的、以中国知识产权为主的、被国际上广泛接受和认可的 3G 标准，主要支持厂商有大唐、华为、中兴等国内著名公司。

8.1.4　无线蜂窝网络的安全性

1. GSM 的安全性

GSM 网络体系结构如图 8.1 所示，由带有 SIM 卡的手持机、基站收发信号台 BTS、基站控制器 BSC、移动交换中心 MSC、认证中心 AuC、归属位置登记数据库 HLR、访问位置登记数据库 VLR 和运营中心 OMC 等部分组成。

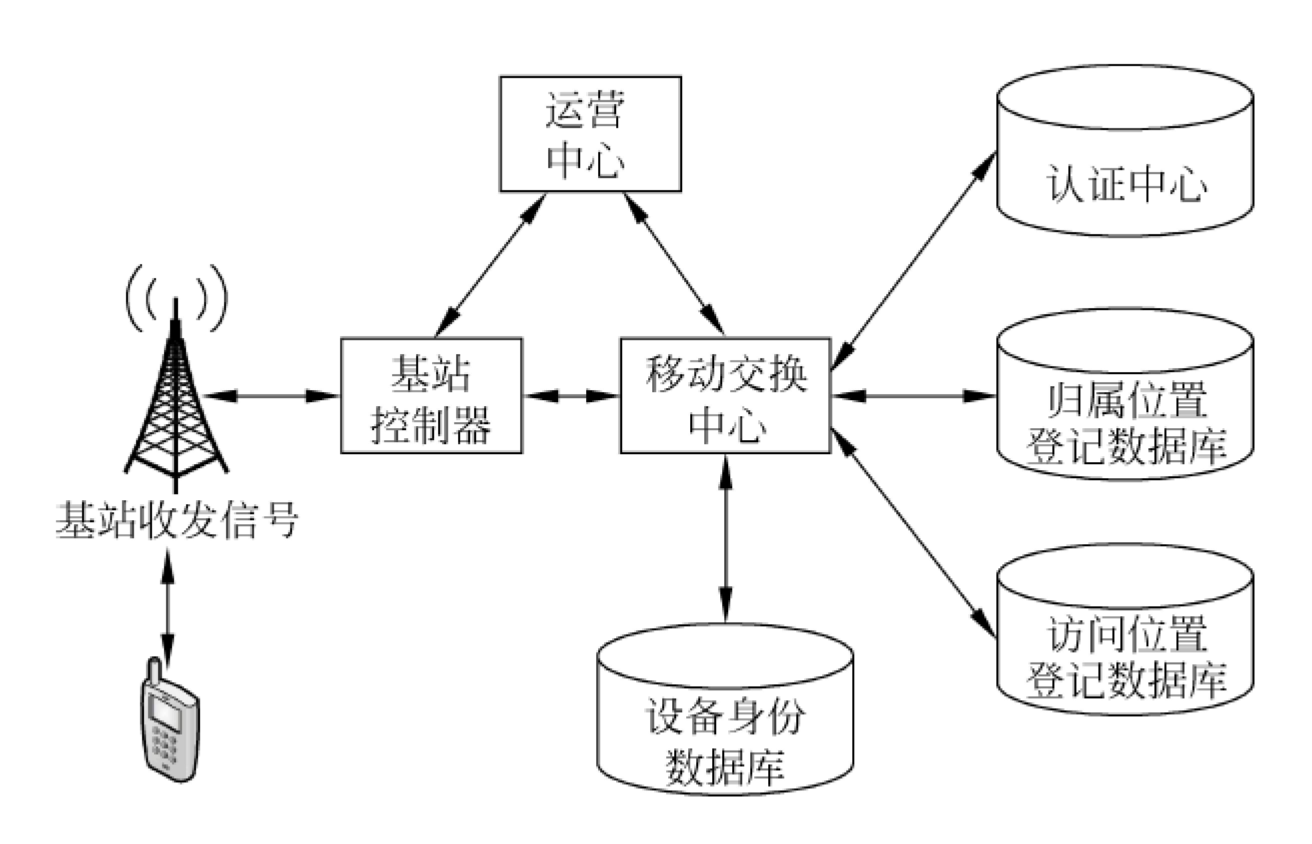


图 8.1 GSM 网络体系结构

（1）GSM 的安全性

GSM 的安全性基于对称密钥的加密体系。GSM 主要使用了 A3、A5 和 A8 三种加密算法。A3 是移动设备到 GSM 网络认证的算法，A5 是认证成功后加密语音和数据的分组加密算法，A8 是产生对称密钥的密钥生成算法。

GSM 安全架构中的第一步是认证，确认一个用户和他的移动设备是授权访问 GSM 网络的。因为 SIM 卡和移动网络具有相同的加密算法和对称密钥，它们可以建立信任关系。在移动设备中，这些信息存储在 SIM 卡中。SIM 卡中的信息由运营商定制（包括加密算法、密钥、协议等），通过零售商分发到用户手中。

根据运营商提供的服务内容，单个用户还可以在 SIM 卡里存储电话号码和短消息。MSC 也保存着 A3、A5 和 A8 算法的副本，通常是存储在硬件设备里。

（2）GSM 的认证过程

当一部手机开始通话时，GSM 网络的 VLR 会立刻与 HLR 建立联系，HLR 从 AuC 获取用户信息。这些信息会转发到 VLR 上，VLR 认证用户的身份。认证过程如下（见图 8.2）：

① 基站产生一个 128 位的随机数或询问数（RAND），并将其发给手机。

② 手机使用 A3 算法和密钥 K_i 将 RAND 加密，产生一个 32 位的签名回应（SRES），同时 VLR 也计算出一个 SRES 值。

③ 手机将 SRES 传输到基站，基站转发到 VLR。

④ VLR 将收到的 SRES 值与计算出的 SRES 值进行对比。

⑤ 如果与 SRES 值相符，认证成功，用户可以使用网络；否则，连接终止，错误信息报告到手机上。

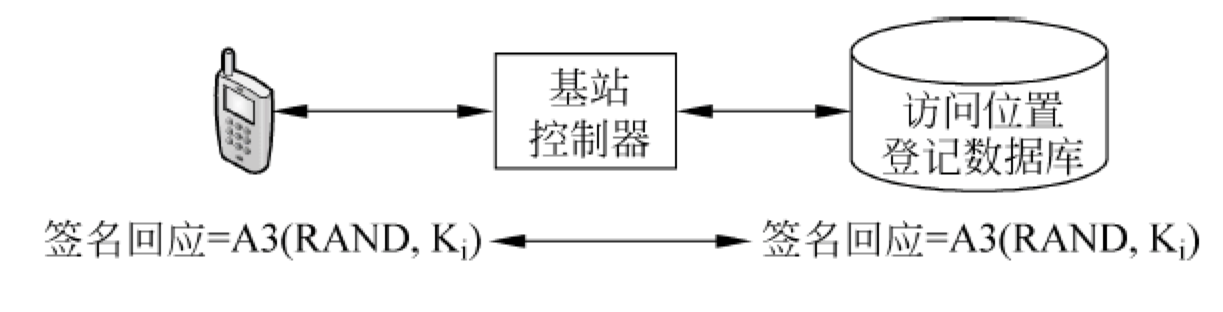


图 8.2 GSM 的认证过程

(3) GSM 的保密性

在成功地认证后，GSM 网络和手机会完成一个建立加密信道的过程。首先需要产生一个加密密钥，然后该加密密钥被用来加密整个通信过程。

① SIM 卡使用 RAND，将它与 K_i 结合在一起，通过 A8 算法生成一个 64 位的会话密钥(K_c)。

② GSM 网络也计算出相同的会话密钥。

③ K_c 与 A5 算法结合在一起，产生手机与 GSM 网络之间的加密通信数据。

2. CDMA 的安全性

CDMA 网络的安全性同样也建立在对称密钥体系上，其网络架构大致与 GSM 相同。

CDMA 手机使用 64 位对称密钥(称为 A-Key)进行认证。购买手机时，这个密钥被程序输入至手机内，同时也由运营商保存。手机内的软件计算出一个校验值，确保 A-Key 正确输入。

(1) CDMA 认证

当用手机打电话时，CDMA 网络的 VLR 对用户进行认证。CDMA 网络使用一种称为蜂窝认证的技术和语音加密(CAVE)的算法。

为了减少 A-Key 被截获的风险，CDMA 手机采用一种基于 A-Key 的动态生成数来进行认证。该生成数称为共享密钥(SSD)，它是由用户的 A-Key、手机的电子序列号(ESN)和随机数 RAND 三个数值计算出来的，如图 8.3 所示。这三个数值通过 CAVE 算法产生一个杂凑值。该 CAVE 操作会生成 SSD_A 和 SSD_B 两个 64 位值。SSD_A 等同于 GSM 的 SRES，用于认证；SSD_B 等同于 GSM 的 K_c，用于加密。

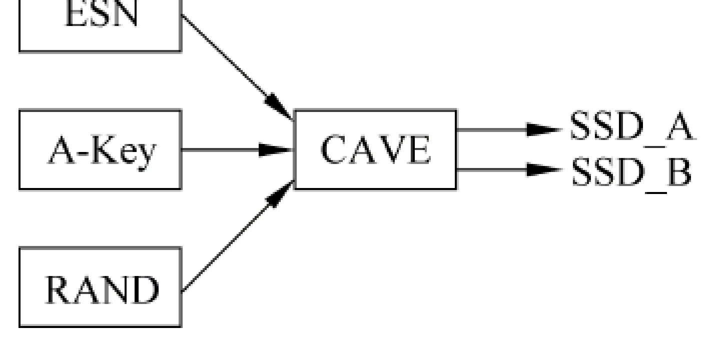


图 8.3　CAVE 算法

当手机处于漫游状态时，SSD_A 和 SSD_B 被明文传输到正在访问的网络中。这可能产生安全风险，因为黑客可以通过截获 SSD 值来复制手机信息。为了预防这种攻击，手机和网络使用一个同步通话计数器。每当手机和网络建立新的通话时，计数器就会更新，这样就能够检测出计数器没有更新的复制 SSD。

CDMA 的认证同样是建立在询问和应答过程上的。认证可以由本地 MSC 或者 AuC 来完成。如果一个 MSC 不能完成 CAVE 计算，认证就由 AuC 来实现。CDMA 的认证过程如下(见图 8.4)：

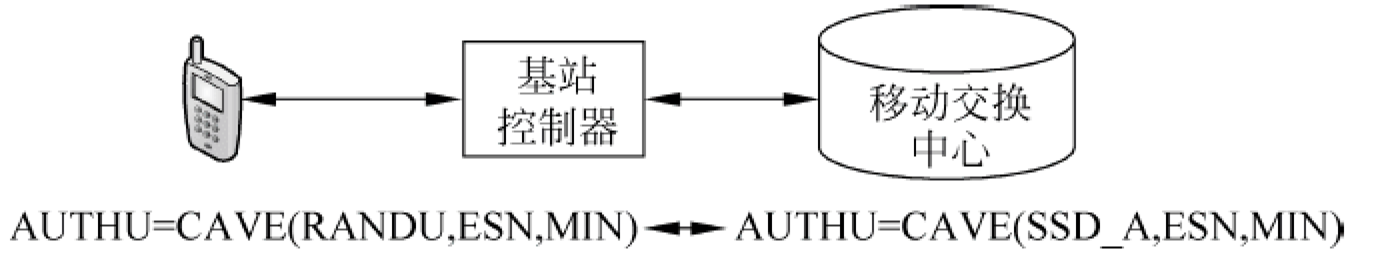


图 8.4　CDMA 的认证过程

① 移动手机拨出电话，MSC 从 HLR 获取用户信息。

② MSC 产生一个 24 位的随机数用于询问(RANDU)，并将 RANDU 传输到手机。

③ 手机收到 RANDU 后，与 ESN 和 MIN 一起用 CAVE 算法生成杂凑值，得到一个 18

位的 AUTHU，并将其传输到 MSC。

④ 同时 MSC 通过 SSD_A、ESN 和 MIN，用 CAVE 计算出自己的 AUTHU。

⑤ MSC 将两个 AUTHU 进行比对，如果两者一致，则继续进行通话；否则，中止通话。

（2）CDMA 的保密性

CDMA 采用与 GSM 类似的语音加密机制。虽然 CDMA 标准允许语音通信加密，但 CDMA 运营商并不总提供这种服务，因为 CDMA 采用的扩频技术和随机编码技术本身就比 GSM 采用的 TDMA 技术保密性好。

CDMA 采用的加密算法与 GSM 一样也是保密的，因此针对 CAVE 算法的攻击很少，但这并不意味着 CAVE 算法本身的强固性，它在理论上很有可能也存在着漏洞。CDMA 正开始逐渐过渡到公开加密算法上，这样会大大加强加密算法的强固性，同时也使 CDMA 运营商能够提供更多的移动商务服务。

3. 3G 的安全性

（1）2G 的安全缺陷

2G 系统主要存在如下安全缺陷。

① 单向身份认证，无法防止伪造网络设备的攻击。

② 加密密钥与认证数据在网络中使用明文传输，易造成信息泄露。

③ 加密功能没有延到核心网，从基站到基站控制器的传输链路中用户信息与信令数据均是明文。

④ 用户身份认证密钥不可变，无法抗击重放攻击。

⑤ 无消息完整性认证，不能保证数据在链路传输过程中的完整性。

⑥ 用户漫游时，服务网络采用的认证参数与归属网络之间没有有效联系。

⑦ 无第三方仲裁功能，当网络各实体间出现纠纷时，无法提交给第三方进行仲裁。

（2）3G 的安全特性

3G 是在 2G 基础上发展起来的，继承了 2G 系统的优点，同时针对 3G 系统的新特性，定义了更加完善的安全特征与安全服务。

3G 系统安全设计充分考虑了 2G 系统存在的安全性缺陷，在结构设计及算法设计中予以克服。3G 系统不仅支持传统的话音与数据业务，还支持交互式业务与分布式业务，从而提供了一个全新的业务环境。这种全新的业务环境不仅体现了新的业务特征，还要求系统能够提供如下的安全特征。

① 存在不同的服务提供商，同时提供多种新业务及不同业务的并发支持。新的 3G 系统安全特征需综合考虑多业务情况下的被攻击性。

② 3G 系统采用固定线路传输。

③ 3G 系统中存在各种预付费业务及对方付费业务，应提供相应的安全保护。

④ 3G 系统的安全特征应能抗击用户可能进行主动攻击。

⑤ 3G 系统中非话音业务将占主要地位，对安全性的要求更高。

⑥ 3G 系统中终端能力进一步增强。

（3）3G 的安全目标

基于上述原则和安全特性，3G 系统安全应达到如下安全目标。

① 确保所有用户产生或与用户相关的信息得到足够的保护，以防止滥用或盗用。
② 确保归属网络与访问网络提供的资源与服务得到足够的保护，以防滥用或盗用。
③ 确保标准安全特性的全球兼容能力。
④ 确保安全特性的标准化，保证不同服务网络间的漫游与互操作能力。
⑤ 确保提供给用户与运营商的安全保护水平高于已有的固定或移动网络。
⑥ 确保 3G 安全能力的扩展性，从而可以根据新的威胁不断扩展安全功能。

8.2　无线局域网安全

无线局域网(WLAN)是利用无线通信技术在一定的局部范围内建立的网络，是计算机网络与无线通信技术相结合的产物，它以无线多址信道作为传输媒介，提供传统有线局域网 LAN 的功能，能够使用户真正实现随时、随地、随意的宽带网络接入。

作为企业网络的一部分，WLAN 越来越受到人们的关注。利用 WLAN，用户可以在建筑物内或大学校园里的任何地方自由地使用笔记本电脑上网。当然，WLAN 也存在着严重的安全问题。它提供给用户的方便也可能成为攻击者侵入网络的捷径。攻击者往往选择 WLAN 作为攻击目标，是因为网络管理员配置时没有考虑安全隐患。

在 WLAN 应用中，对于家庭用户、公共场景安全性要求不高的用户，使用 VLAN(虚拟局域网)隔离、MAC 地址过滤、服务区域认证 ID(ESSID)、密码访问控制和有线等效保密(wired equivalent privacy，WEP) 协议可以满足其安全性需求。但对于公共场所中安全性要求较高的用户，仍然存在着安全隐患，需要将有线网络中的一些安全机制引进到 WLAN 中。在无线访问点(access point，AP)实现复杂的加密解密算法，通过无线接入控制器，利用 PPPoE 或 DHCP Web 认证方式对用户进行认证，对用户的业务流实行实时监控。

常见的 WLAN 连接标准是 IEEE 802.11 协议。802.11 规范仅仅定义了无线以太网的物理层和 MAC 地址部分。802.11 协议中包含了三个不同的物理层标准：802.11b、802.11a 和 802.11g，这些协议对应着实现 802.11 标准的不同方法。

802.11a 标准工作在 5GHz 频段，有 8 个射频信道用于数据传输。802.11a 适配卡支持的数据传输率高达 54Mb/s。因为 802.11a 和 802.11b 适配卡工作在不同频段，所以二者不兼容。802.11g 工作在 2.4GHz 和 5.0GHz 两个频段，但速率与 802.11a 标准一样，可达 54Mb/s。

WLAN 面临的基本安全问题与 WWAN 一样，攻击者发起攻击将不再受必须在建筑物内部连接网络端口等限制。无线攻击时也不受相应的物理限制，也不必设法绕过路由器、防火墙和服务器安全系统等网络边界安全措施。攻击者可在网络内部发起攻击，因为那里障碍较少，更易成功。

8.2.1　访问点安全

WLAN 的安全应从访问点着手，保护访问点要采取的措施是场地安全。访问点必须从物理上加以保护，使攻击者不能容易地访问。

访问点应位于靠近建筑物的中心，这样当信号到达边界时就变得弱了。假设一个机构

有多个建筑物，准备建立覆盖整个园区的 WLAN，要把信号限制在建筑物的内部可能很困难，就要采取措施来确保园区自身的安全，阻止未经授权的用户进入该地区。

如果访问点上存储有密钥和其他的过滤器，访问它们将受到限制。这就对大多数 WLAN 管理员提出了一个实际的问题，因为许多访问点配有管理工具，这些管理工具有先天的不安全性。访问点通常依靠 HTTP、Telnet 和 SNMP 技术来配置。Telnet 和 HTTP 的安全缺陷是所有数据都是明文发送，而 SNMP、Telnet 和 HTTP 都面临许多同样的安全问题。

只要可能，在访问点上应该禁用 HTTP、Telnet 和 SNMP 功能，并使用其他的安全访问技术（如 HTTPS 或 SSH）。如果厂商不支持对访问点控制的安全技术，那么到访问点的连接就只能通过有线网段进行。

应定期地扫描所有访问点查找未经授权的（访问）通信，更重要的是查找未经授权的访问点。因为偶尔企业用户或用户组可能在实验室建立 WLAN 而没有通知 IT 管理部门，这些用户对安全保护 WLAN 的必须步骤并不知晓，因而可能会不经意地允许未经授权的通信访问网络。

通常，有线网络的安全措施可以阻止未经授权的访问点连接 WLAN 到网络。可以在配有 802.11b 局域网卡的手持设备上安装 IBM 的 Wireless Security Auditor 和 Netaphor Software 的 PDAlert 软件产品来监视网络活动。这些软件产品特别设计用来审计 WLAN 网络和警告管理员注意潜在的安全漏洞。

8.2.2 无线局域网协议安全

1. SSID

像其他类型的安全一样，WLAN 安全包括很多层次。有些层次是可选的，为保障 WLAN 的安全性，应实现尽可能多的安全保护层。

第一个安全层是服务设置标识符（SSID）。SSID 基本上是一个连接到访问点时客户端必须提交的口令。如果客户端传送的 SSID 能与访问点上的合法口令匹配，即可建立连接，开始通信。

SSID 也是分割无线网络的好方法。如果一个校园网设计成用户只能访问网络的特定部分，那么可以在不同的区域使用不同的 SSID，以便限制用户对网络特定部分的访问。

2. WEP

WEP 协议是对在两台设备间无线传输的数据进行加密的技术，可用以防止非法用户窃听或侵入无线网络。对多数管理员来说，SSID 本身没有提供足够的安全。为进一步保护 WLAN，许多管理员会使用 WEP 协议。

WEP 是 802.11 标准的部分封装形式，它使用对称密钥加密体系来保护终端用户和访问点之间的数据。WEP 标准指定用 RC4 伪随机数生成（PRNG）算法来加密两设备间传输的密钥。密钥在 WLAN 网卡和访问点上都有存储，且网卡和访问点之间传输的所有数据都用该密钥加密。802.11 标准不提供密钥管理功能，所有的密钥都要人工管理。

WEP 协议不允许多密钥绑定在一个访问点上。因此，所有用户有同样的绑定在网卡上

的密钥,而每个访问点仅有一个密钥。WEP 密钥的使用允许管理员限制哪些用户使用特定访问点进入网络。不同的密钥与不同的访问点或访问点组相关,但所有授权使用同一个访问点的用户必须在他们的 WLAN 网卡上设置相同的密钥。WEP 封装存在严重的安全缺陷。攻击者使用像 AirSnort 这样的程序,可以嗅探到足够的信息,只需要 500MB 的数据就可以攻破 WEP 封装。WEP 密钥的更新需要口头或通过加密邮件通知各个用户,当新的密钥发挥作用后,包含该密钥的信息应该被删除。由于 WEP 没有提供足够的安全,因而不适合作为一种数据保护的独立方法。它与非广播 SSID 形成的组合协议加密可提供更高级别的安全,但组合协议也不能为企业网络提供足够的安全。

3. MAC 地址过滤

在 WLAN 上使用的另一个安全层是 MAC 地址过滤,就像管理员在交换式网络上可以过滤 MAC 地址一样,在 WLAN 网络上也可以过滤 MAC 地址。在管理员可以保护安全的小型 WLAN 中,MAC 地址过滤才有意义。

MAC 地址也可能被欺骗。在 WLAN 中,攻击者可以不经访问点验证就监视通信,即使是加密的数据,连接到网络机器的 MAC 地址也以明文发送。嗅探者就能够发现经允许的 MAC 地址,并且修改他们正在使用的网卡的 MAC 地址来获得网络的快速入口。

目前最好的方法就是联合使用非广播的 SSID、WEP 和 MAC 地址过滤方法来保护 WLAN。即使这些措施不足以提供像有线网络那样的安全水平,但对小型 WLAN 来说,这些措施已足够了。

4. RADIUS 验证

配置访问点使用 RADIUS 对用户进行验证可以进一步增强无线网络的安全。RADIUS 验证给管理员提供通过 WLAN 访问点访问网络的更多精细粒度的控制,并不是所有的访问点都支持 RADIUS 验证,但像 Cisco、Linksys、Lucent 和 Proxim 等著名供应商的访问点都支持 RADIUS 功能。Funk Software 的 RADIUS 软件含有支持无线 RADIUS 验证的特殊扩展。

RADIUS 的验证过程如图 8.5 所示,RADIUS 服务器迫使 WLAN 用户在获得网络访问前进行验证。用户连接到访问点,使用 SSID、WEP 或两者来进行网卡验证。访问点向 RADIUS 服务器提交 RADIUS 请求,RADIUS 服务器验证现在能够传送网络通信的用户。为保证可靠性,访问点还可以增加一个 RADIUS 备用服务器。如果主服务器失效,用户将自动转发给备用服务器。

RADIUS 验证阻止未授权的用户通过 WLAN 访问网络。如果用户不能通过 RADIUS 服务器验证,就不允许访问网络。当用在强密码策略的连接中,RADIUS 验证有助于制止未授权用户获得对网络资源的访问。

5. WLAN VPN

在 WLAN 中添加 VPN 隧道可以提供验证和加密。要求通过 VPN 访问 WLAN 是新的安全方法,正在获得广泛支持。

WLAN VPN 是通过在网络和访问点之间加装 NAS 服务器实现的,如图 8.6 所示。使

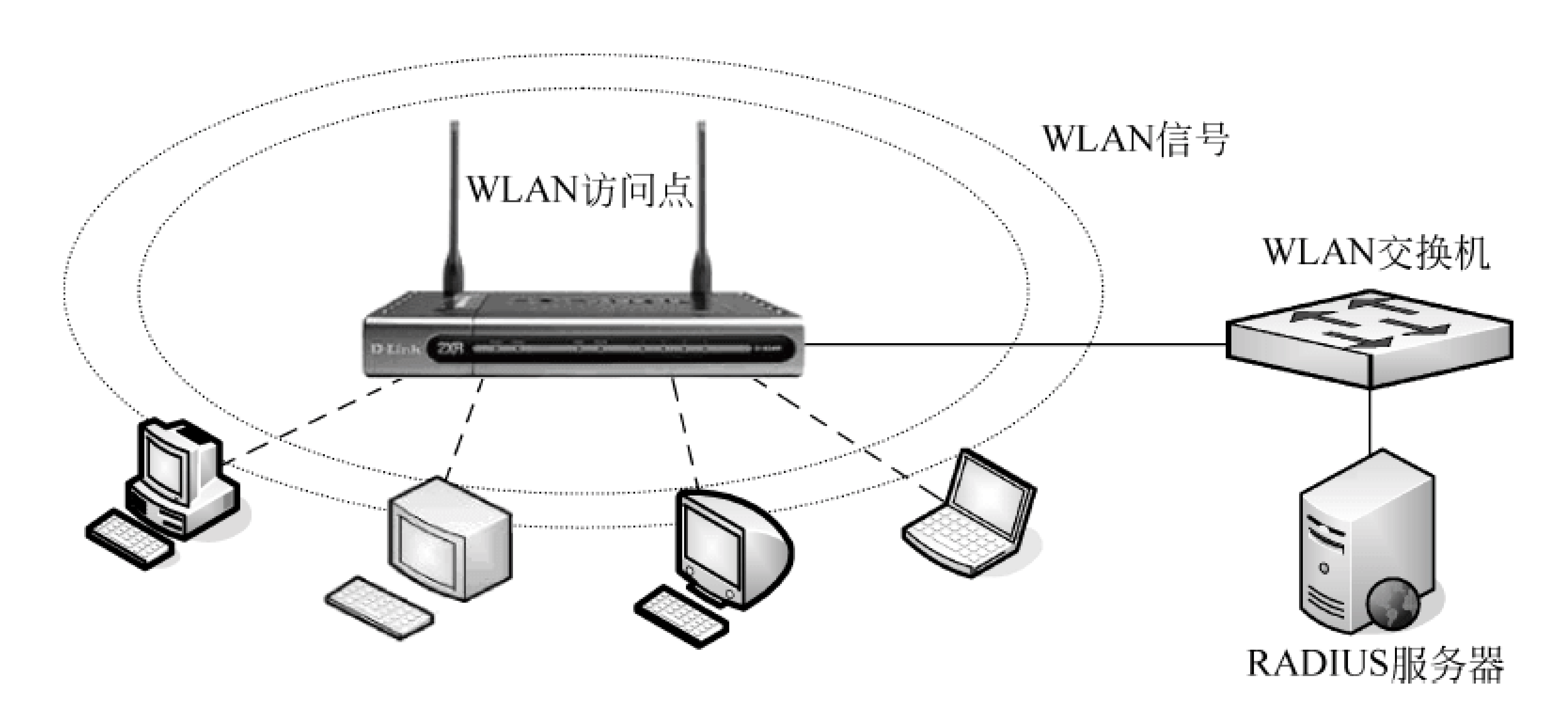


图 8.5 使用 RADIUS 验证 WLAN

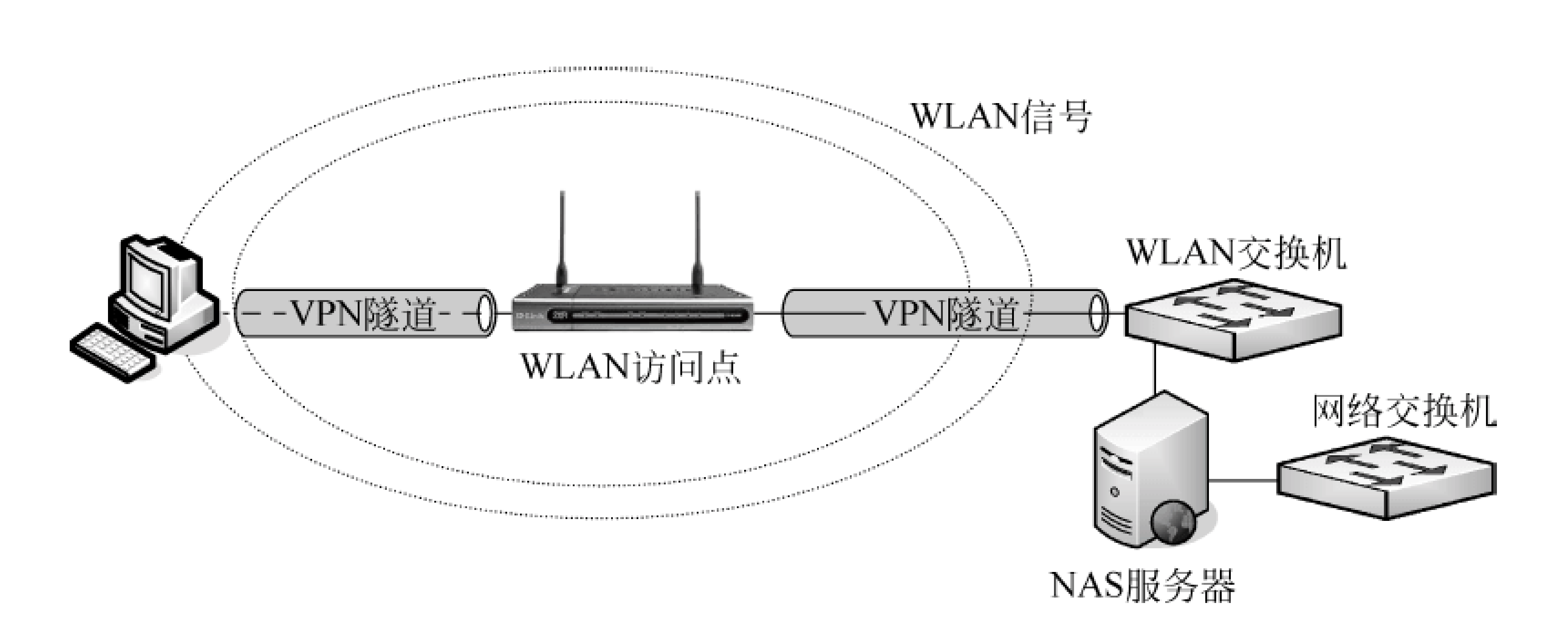


图 8.6 使用 VPN 保护 WLAN

用 VPN 保护 WLAN，WLAN 用户建立通向访问服务器的隧道，加密所有在用户和网络间传输的通信。WLAN 用户连接访问点，请求转发给 NAS。NAS 处理数据加密和验证，并创建隧道。一旦用户成功地通过 NAS 服务器的验证，隧道就建立了，加密的数据就可以在用户和网络间自由地传输。

WLAN VPN 的优势之一是多数操作系统都支持 VPN 隧道的普通客户端（如 PPTP、L2TP 和 IPSec）。

尽管 WLAN VPN 技术很好，且许多人认为是企业网络的关键，但它仍然存在一些不足。如在 NAS 服务器和终端用户机器上都要建立隧道，需要额外的 CPU 开销。如果网络上没建立 VPN，那么建立新的 VPN 还要花费很多时间和费用。

6. IEEE 802.11i

为了进一步加强无线网络的安全性和保证不同厂家之间无线安全技术的兼容，IEEE 802.11i 工作组开发了作为新的安全标准 IEEE 802.11i，并且致力于从长远角度考虑解决 IEEE 802.11 无线局域网的安全问题。IEEE 802.11i 标准中主要包含加密技术 TKIP (temporal key integrity protocol，暂时密钥集成协议)、AES(advanced encryption standard，高级加密标准)和认证协议 IEEE 802.1x。

(1) TKIP

TKIP 设计成向后兼容 WEP，并且允许厂商提供对硬件产品的固件升级。这意味着公

司将可以在现有设备上运行 TKIP，而不必购买所有新的设备。TKIP 与 WEP 一样基于 RC4 加密算法，TKIP 将 WEP 密钥的长度由 40 位加长到 128 位，初始化向量的长度由 24 位加长到 48 位，并对现有的 WEP 进行了改进。TKIP 实际是封装 WEP 会话信息的一种方式，用于解决与 WEP 有关的伪数据包、转播攻击、弱密钥和密钥的重新生成等安全问题。

802.11i 工作组为 TKIP 开发了一种对每个数据包都加密钥的新方法。TKIP 使用一个两阶段的密钥生成过程，第一个阶段是将 WLAN 网卡的 MAC 地址和一个暂时密钥结合起来生成中间密钥，第二个阶段将中间密钥下的每个数据包的序列号加密生成一个 128 位的密钥。因为暂时密钥的生命期(TTL)短，在这个过程重新开始之前，加密只使用很短的时间，因此攻击者要解开密钥就非常困难。

TKIP 对 WEP 进行的改进之一是对加密密钥的管理。TKIP 过程使用 3 种不同的密钥：暂时密钥、加密密钥和管理员主密钥。因为当 WLAN 设备和访问点连接或重新连接时每种密钥都必须重置，为监视这个过程，TKIP 使用重加密密钥报文。重加密密钥报文保证无论是 WLAN 设备还是访问点都不能重新生成前面通信中使用的密钥。

(2) AES

802.11i 工作组开发的第二种封装形式是基于 AES 的。因为 AES 加密涉及更多的额外操作，它与现存的大多数设备不兼容。

AES 又称为 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。AES 是美国政府 2001 年 11 月公布的加密标准，用来替代原先的 DES，已经被多方分析且广为使用，到 2006 年已成为对称密钥加密中最流行的算法之一。AES 达到了与 TKIP 同样的安全标准，并提供更高级别的加密。

像 TKIP 一样，AES 是一种对称密钥密码，即加密和解密使用相同的密钥。AES 支持长度高达 256 位的密钥，该长度是 TKIP 所支持密钥长度的两倍。AES 以 128 位数据为组加密长度，当数据包大小不是 128 位的倍数时，就填充空位补足。

(3) IEEE 802.1x 认证

IEEE 802.1x 体系包括客户端、认证系统和认证服务器三个实体。客户端是接收认证的客户端，如 WLAN 终端(STA)。在无线网络中认证系统就是无线接入点或具有无线接入点功能的通信设备，其主要作用是完成用户认证信息(802.1x 报文)在客户端和认证服务器之间的传递，控制用户是否可以接入到网络中。一般普遍采用 RADIUS 作为认证服务器，它可检验客户端的身份是否合法，通知认证系统是否可以让客户端接入。

IEEE 802.1x 并不是专为 WLAN 设计的，它已经在有线网络中被广泛应用。使用这个成熟的认证体系，确保 WLAN 安全建立在一个成熟的基础之上，实现了有线和无线共用认证体系。为了适应 WLAN 的特点，IEEE 802.11i 对 IEEE 802.1x 进行了增强补充，包括支持 EAPOL-Key 的协商过程等，以帮助完成设备端和客户端进行动态密钥协商和管理。

IEEE 802.1x 比较适合企业应用环境。考虑到家庭等用户不需要部署 RADIUS 来实现用户身份认证，所以 802.11i 还定义了预共享密钥，以便让用户直接在 WLAN 设备和无线终端上配置 PMK(pairwise master key)。

8.3 无线网络的安全配置实践

8.3.1 无线网络路由器配置

把路由器接入无线网络并与计算机连接在一起后，可通过路由器的管理界面对路由器进行配置。

1. WAN 无线路由器的基本配置

现以 TP-LINK WR340G 路由器为例介绍无线路由器的配置，过程如下：

第 1 步：打开 IE 浏览器，在“地址栏”输入 192. 168. 1. 1，按回车键后会弹出一个要求输入用户名和密码的对话框，输入用户名和密码，如图 8.7 所示。

第 2 步：单击“确定”按钮后，进入 TP-LINK WR340G 路由器管理主界面，如图 8.8 所示。路由器管理主界面左侧是一系列管理选项，通过这些选项，可以对路由器的运行情况进行管理和控制。



图 8.7 登录窗口



图 8.8 TL-WR340G 路由器管理主界面

第 3 步：第一次进入路由器管理界面，或在路由器管理主界面单击左侧菜单中的“设置向导”选项，会弹出一个“设置向导”对话框，如图 8.9 所示，单击“下一步”按钮，进入设置向导。

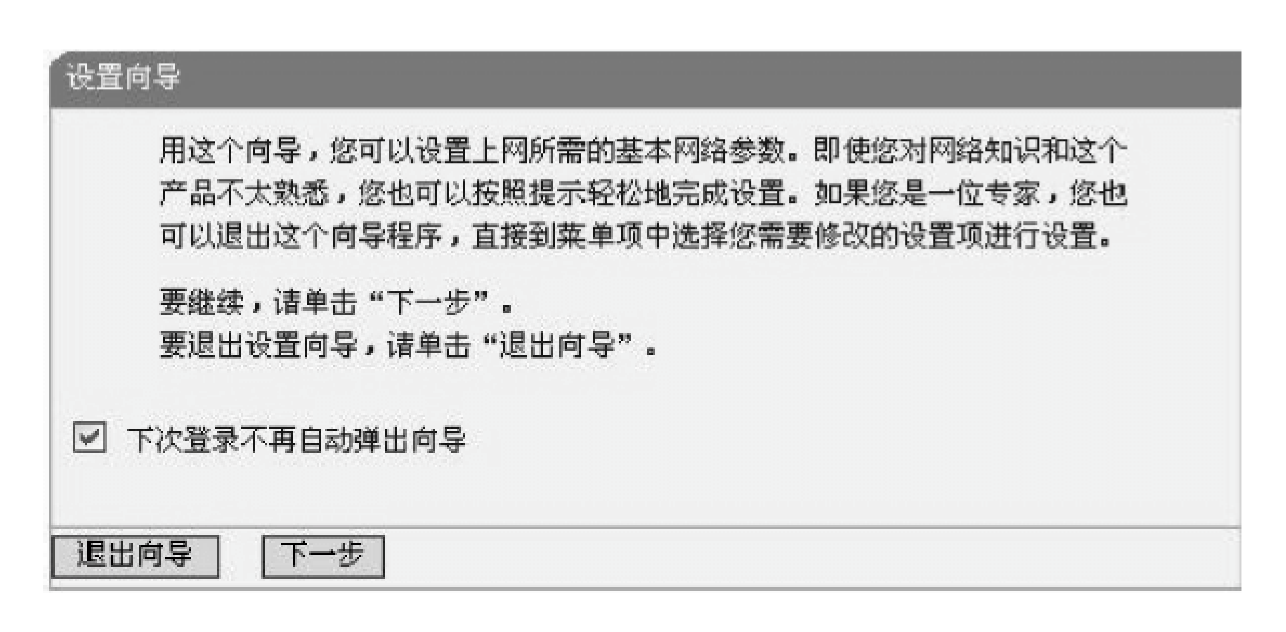


图 8.9　“设置向导”对话框

第 4 步：WAN 口设置。在弹出的如图 8.10 所示的“WAN 口设置”对话框中，用户需要按实际情况选择使用的上网方式，这是极为重要的一步。在“WAN 口连接类型”的下拉列表框中，选择 PPPoE 选项，在“上网账号”和“上网口令”文本框中分别输入对应的用户名和密码。由于 ADSL 可以自动分配 IP 地址和 DNS 服务器，所以这两项都不用填写。直接在对应连接模式中，选择“自动连接”选项，这样一开机就可以连入网络，大大提高了效率。设置完成后，单击“保存”按钮保存设置内容。

WAN口连接类型：PPPoE
上网账号：useradsl
上网口令：●●●●●●●●●●●●●
如果正常拨号模式下无法连接成功，请依次尝试下列模式中的特殊拨号模式：
正常拨号模式
特殊拨号模式1
特殊拨号模式2
根据您的需要，请选择对应的连接模式：
按需连接，在有访问时自动连接
自动断线等待时间：15 分（0 表示不自动断线）
自动连接，在开机和断线后自动连接
定时连接，在指定的时间段自动连接
注意：只有当您到“系统工具”菜单的“时间设置”项设置了当前时间后，“定时连接”功能才能生效。
连接时段：从 0 时 0 分到 23 时 59 分
手动连接，由用户手动连接
自动断线等待时间：15 分（0 表示不自动断线）
连 接　断 线
高级设置
保 存　帮 助

图 8.10　“WAN 口设置”对话框

在此需要说明的是，如果不是包月用户，推荐使用“手动连接”，避免网费超支。

第 5 步：路由器的 DHCP 功能设置。DHCP 是路由器的一个特殊功能，使用 DHCP 可以避免因手工设置 IP 地址和子网掩码所产生的错误，也可避免把一个 IP 地址分配给多台客户机所造成的地址冲突。使用 DHCP 不但能大大缩短配置或重新配置网络中客户机所花费的时间，而且通过对 DHCP 服务器的配置，还能灵活地设置地址的租期。

单击图 8.8 所示管理主界面左侧的“DHCP 服务器”选项，弹出“DHCP 服务”对话框，如图 8.11 所示。单击“启用”选项，“地址池开始地址”和“地址池结束地址”选项分别为 192.168.1.X 和 192.168.1.Y(X<Y，X 不能是 0 和 1，Y 不能是 255)，在此输入确定 X、Y 后的 IP 地址。设置完毕后，单击“保存”按钮。

在进行上述设置后，只要打开网络中的任何一台计算机，启动 IE 浏览器，就可以上网了。

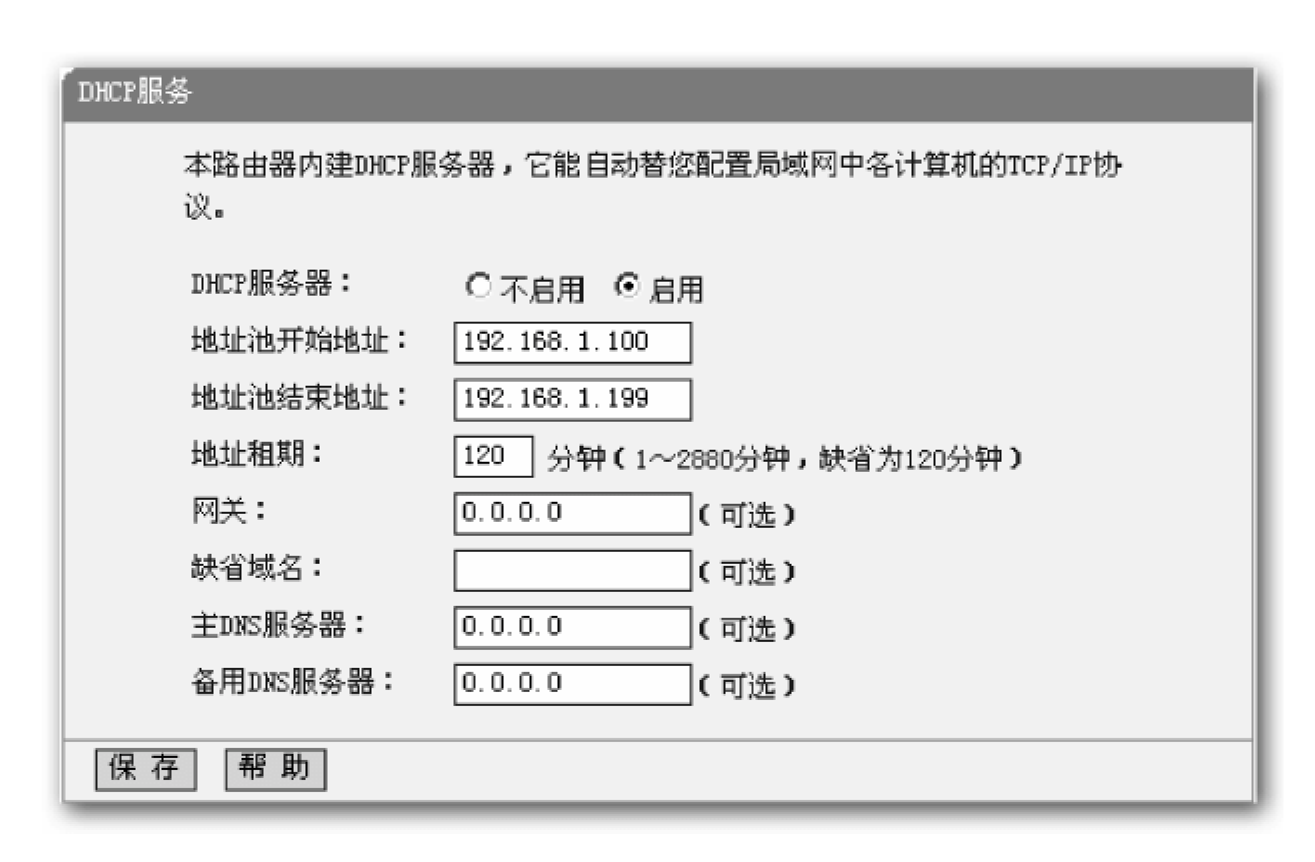


图 8.11　“DHCP 服务”对话框

2. LAN 无线路由器配置

现以 TP-LINK TL-WR541G(局域网无线宽带路由器)为例介绍 WLAN 路由器的配置。该配置实践主要分为设备选取和参数配置两大过程。无线网卡选取的是 TL-WN510G/550G/610G/650G 系列产品。

第 1 步：将电脑 IP 设成 192.168.1.3，子网掩码设成 255.255.255.0，网关为 192.168.1.1。在 IE 中输入 http://192.168.1.1，按回车键后进入如图 8.7 所示的管理员登录界面。TP-LINK 设备的用户名和密码一般都是 admin。单击“确定”按钮后，进入如图 8.12 所示 TL-WR541G 路由器管理主界面。



图 8.12　TL-WR541G 路由器管理主界面

第 2 步：由此可容易地设置 LAN 口参数，如图 8.13 所示。

图 8.13　“LAN 口设置”对话框

第 3 步：设置无线参数。进入 TL-WR541G 后在“无线网络基本设置”界面默认配置，如图 8.14 所示。

图 8.14　“无线网络基本设置”对话框

选择无线参数，基本设置有 SSID 号、频段、模式默认，开启无线功能，允许 SSID 广播等项。各参数含义如下：

- SSID 号：用于识别无线设备的服务集标志符。无线路由器就是用该参数来标识自己，以便无线网卡区分不同的无线路由器连接。该参数是由无线路由器来决定而不是由无线网卡决定的。如无线网卡周围有 A 和 B 两个无线路由器，分别用 SSID A 和 SSID B 标识，这时候无线网卡如何连接，则要通过 SSID 标识符来分辨。这里默认 SSID 就是 TP-LINK。
- 频段：用于确定本网络工作的频率段，选择范围为 1～13，默认为 6。要注意的是：假设相邻用户也使用无线网络，且同样使用频道 6，则为了减小两个无线路由器之间的无线干扰，可以考虑将这个参数更改为 1 或 13 都可以。
- 模式：该参数用来设置无线路由器的工作模式，这里有 54Mb/s（802.11g）和 11Mb/s（802.11b）两个可选项，一般选择默认参数。
- 开启无线功能：使 TL-WR541G 的无线功能打开和关闭。
- 允许 SSID 广播：默认情况下无线路由器都是向周围空间广播 SSID 通告自己的存

在，这种情况下无线网卡都可以搜索到该无线路由器的存在。如果将该复选框里的勾去掉，也就是无线路由器不进行 SSID 的广播，此时无线网卡就无法搜索到无线路由器了。

在确定以上默认设置后，给 TL-WR541G 加电时，就会在 TL-WR541G 周围生成一个无线网络，这个网络的 SSID 标识符就是 TP-LINK，工作信道是 6，网络没有加密。这时一个没有加密的无线网络就存在于 WR541G 周围了，可以提供给无线网卡来连接。

第 4 步：因企业内部网有 DHCP 服务器，因此将此无线路由器的 DHCP 功能关闭。

第 5 步：设置远程 Web 管理端口及用户登录密码。

8.3.2 无线路由器的防火墙功能设置

使用路由器，用户可以对局域网内部各客户机的上网情况进行监控和管理。通过开放不同的权限，可以控制某些计算机屏蔽某些网站和 E-mail。利用路由器的防火墙功能即可对网络进行安全和监控管理。

下面介绍路由器的防火墙功能设置，帮助网络管理员实现路由器的监管功能。

单击图 8.8 所示路由器管理主界面左侧的“安全设置”选项，在展开的菜单中选择“防火墙设置”，打开如图 8.15 所示的“防火墙设置”对话框。这是一个总开关的设置页面，凡是不用的功能就不要勾选，在可选项里打勾表示开启了该功能。

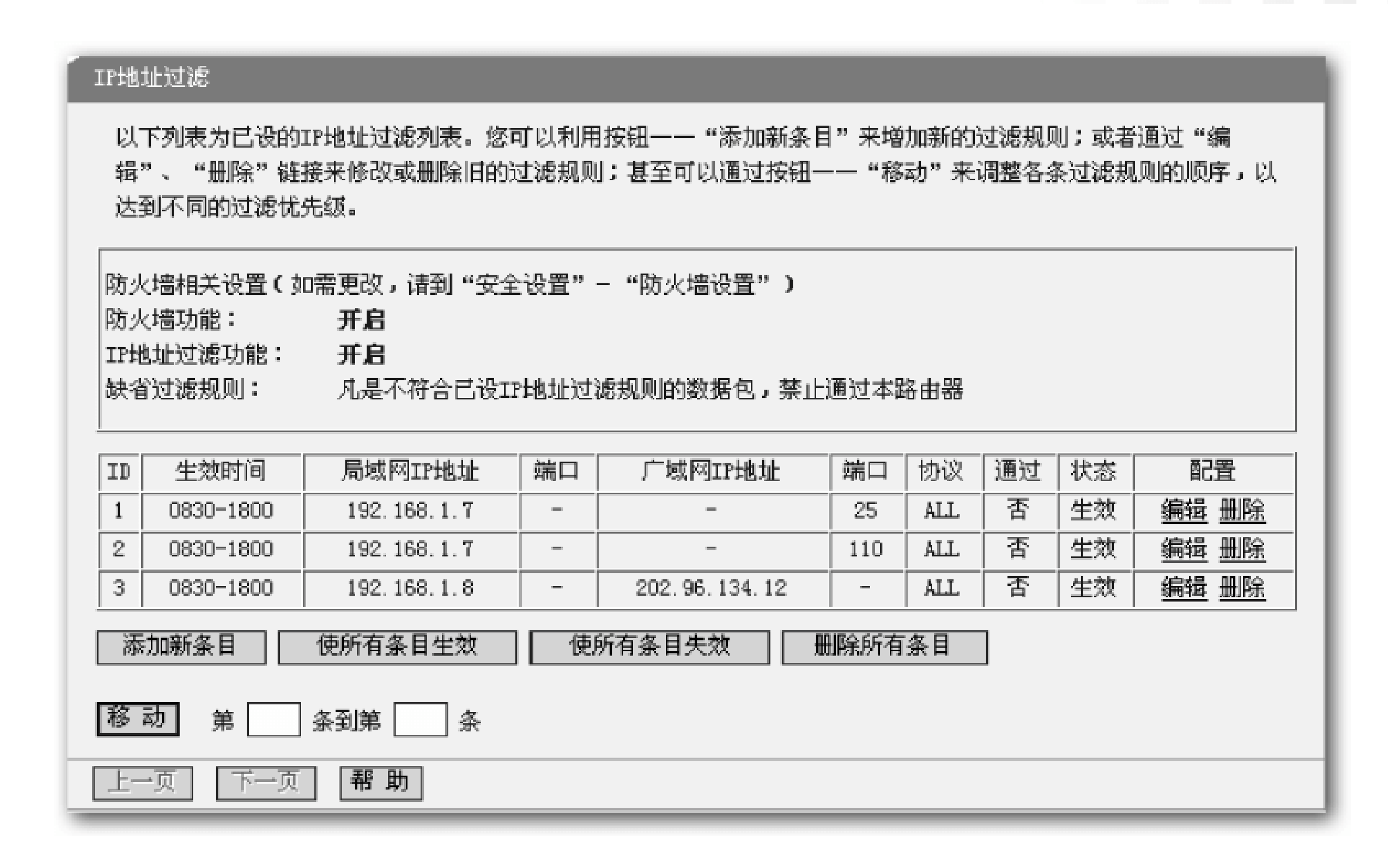


图 8.15 “防火墙设置”对话框

“防火墙的总开关”下方是几个路由器的过滤功能项，其中含有两个“缺省过滤规则”。

1. IP 地址过滤

图 8.16 所示是“IP 地址过滤”设置页面，用户可以对“缺省过滤规则”进行添加。单击“添加新条目”按钮，进入具体的规则设置页面。在该页面中，可以限制 IP 地址是 192.168.1.7 的计算机只能登录 www.tp-link.com.cn 网站，而不能登录别的网站。



IP地址过滤

以下列表为已设的IP地址过滤列表。您可以利用按钮——“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则；甚至可以通过按钮——“移动”来调整各条过滤规则的顺序，以达到不同的过滤优先级。

防火墙相关设置（如需更改，请到“安全设置”－“防火墙设置”）
防火墙功能：　开启
IP地址过滤功能：　开启
缺省过滤规则：　凡是不符合已设IP地址过滤规则的数据包，禁止通过本路由器

ID	生效时间	局域网IP地址	端口	广域网IP地址	端口	协议	通过	状态	配置
1	0830-1800	192.168.1.7	-	-	25	ALL	否	生效	编辑 删除
2	0830-1800	192.168.1.7	-	-	110	ALL	否	生效	编辑 删除
3	0830-1800	192.168.1.8	-	202.96.134.12	-	ALL	否	生效	编辑 删除

添加新条目　使所有条目生效　使所有条目失效　删除所有条目

移动　第　条到第　条

上一页　下一页　帮助

图 8.16　“IP 地址过滤”对话框

在“局域网 IP 地址”后输入要限制的计算机的 IP 地址 192.168.1.7，在“广域网 IP 地址”后输入 www.tp-link.com.cn 域名所对应的公网 IP 地址，如 219.134.132.21。“协议”默认为 ALL，“通过”默认为禁止。因为默认过滤规则是禁止不符合设定规则的数据包通过路由器，所以符合设定规则的数据包允许通过。“状态”则设为生效，设置后“保存”起来，如图 8.17 所示。

IP地址过滤

本页添加新的、或者修改旧的IP地址过滤规则。

生效时间：0830 - 1800
局域网IP地址：192.168.1.7 -
局域网端口： -
广域网IP地址： -
广域网端口：25 -
协 议：ALL
通 过：禁止通过
状 态：生效

保存　返回　帮助

图 8.17　“IP 地址过滤”对话框

保存后，设置好的规则就会显示在过滤规则条目中，可以通过单击其后的“修改”和“删除”对其运行状态进行调整，如图 8.18 所示。

ID	生效时间	局域网IP地址	端口	广域网IP地址	端口	协议	通过	状态	配置
1	0830-1800	192.168.1.7	-	-	25	ALL	否	生效	编辑 删除
2	0830-1800	192.168.1.7	-	-	110	ALL	否	生效	编辑 删除
3	0830-1800	192.168.1.8	-	202.96.134.12	-	ALL	否	生效	编辑 删除

图 8.18　IP 过滤规则列表

2. 域名过滤

在图 8.18 中“开启域名过滤”前打勾并保存，在“域名过滤”页面就可以对要过滤的域名进行添加了，如图 8.19 所示。如果要禁止内部局域网接收 hotmail 邮件，可以进行以下操作。



图 8.19 “域名过滤”对话框

第 1 步：单击“添加新条目”按钮，进入具体的规则设置页面。

第 2 步：在“域名”框输入 hotmail 的域名，“状态”选择生效，单击“使所有条目生效”按钮确认设置条目后，就可以在“域名过滤”页面看到设置好的规则了。此后，在局域网中的计算机就不能再登录 hotmail 接收邮件了。

3. MAC 地址过滤

在图 8.15 中“开启 MAC 地址过滤”前打勾并保存，可进入 MAC 地址过滤页面。MAC 地址过滤和域名过滤功能设置过程基本相同，都是先打开该功能，填入要过滤的项，并启用相应规则，即可限制对有些网站（域名）的访问，如暴力网站、不健康网站等。

习题和思考题

一、问答题

1. 什么是扩频技术？什么是 3G 技术？3G 技术有哪些标准？
2. 简述 3G 的安全目标。
3. CDMA 的主要特点是什么？

二、填空题

1. 无线广域网的主要支持技术有(　　)技术、(　　)技术、(　　)技术和 WEP。
2. 保护传送中的无线数据安全的最好办法是进行(　　)。
3. 我国的 GSM 标准有(　　)和(　　)两个频段。
4. WEP 协议是对在两台设备间无线传输的数据进行(　　)的技术，可用以防止非法用户窃听或侵入无线网络。

5. IEEE 802.11i 标准中主要包含加密技术(　　)、(　　)和认证协议(　　)。

三、单项选择题

1. TD-SCDMA 是(1)(　　)技术,CDMA 是(2)(　　)技术,GSM 是(3)(　　)技术,GPRS 是(4)(　　)技术。

(1) A. 1.5G　　B. 2G　　C. 2.5G　　D. 3G

(2) A. 1.5G　　B. 2G　　C. 2.5G　　D. 3G

(3) A. 1.5G　　B. 2G　　C. 2.5G　　D. 3G

(4) A. 1.5G　　B. 2G　　C. 2.5G　　D. 3G

2. 以下(　　)项是 3G 技术提供的安全性特征。

A. 用户身份认证密钥不可变　　B. 无消息完整性认证

C. 多种新业务及不同业务的并发支持　　D. 单向身份认证

四、实验题

无线 LAN 配置实验:参考相关设备的使用手册,对 WLAN 路由器、路由器的防火墙功能和无线网卡进行配置。

第 9 章 电子邮件安全与应用实践

电子邮件已成为人们日常生活和工作中不可缺少的工具和手段。随着 Internet 的发展和电子邮件的广泛应用，垃圾邮件、邮件炸弹、邮件病毒等影响邮件安全的事件屡屡发生，因此电子邮件的安全问题也突显出来，受到人们的广泛关注。

电子邮件的安全问题主要包括两个方面：一方面是电子邮件服务器的安全，包括网络安全和如何从服务器端防范垃圾邮件、病毒邮件和钓鱼邮件等，这是电子邮件服务的基本要求；另一方面是如何确保用户的电子邮件内容不被窃取、篡改和防止非法用户登录合法用户的电子邮件账号。

9.1 电子邮件的安全漏洞与威胁

电子邮件服务十分脆弱，用户向另一个人发送 E-mail 时，不仅信件像明信片一样是公开的，而且也不知道在到达目的地之前，信件经过了多少节点。E-mail 服务器向全球开放，它们很容易受到黑客的袭击；Web 提供的阅读器也容易受到类似的侵袭。Internet 像一个蜘蛛网，E-mail 到达收件人之前，会经过很多机构和 ISP，因此任何人，只要可以访问这些服务器或访问 E-mail 经过的路径，就可以阅读这些信息。E-mail 存在如下一些安全漏洞。

1. 电子邮件病毒

电子邮件病毒实际上与普通病毒一样，只不过是因为传播途径主要是通过电子邮件。邮件病毒通常是被附加在邮件的附件中，当用户打开邮件附件时，它就侵入了用户计算机。如今，电子邮件也正成为病毒传播的主要途径之一。由于恶意者可同时向多个用户或整个计算机系统群发电子邮件，一旦一个站点感染病毒，病毒邮件就会在短时间内大规模地复制和传播，因此整个系统就会迅速感染，从而可能导致邮件服务器资源耗尽，并严重影响网络运行。部分病毒甚至可能破坏用户本地硬盘上的数据和文件。

电子邮件病毒的传播速度快，传播范围广，绝大多数电子邮件病毒都有自我复制能力。电子邮件中的木马病毒，一旦被打开并运行就可能破坏主机系统的数据或将计算机变成可被远程控制的“肉鸡”，甚至导致收件人经济上的巨大损失。

2. 电子邮件炸弹

电子邮件炸弹是指发送者以来历不明的邮件地址，重复地将电子邮件邮寄给同一个收

信人。由于这就像战争中利用某种战争工具对同一个地方进行狂轰滥炸一样，因此称为电子邮件炸弹。这种以重复的信息不断地进行的电子邮件轰炸操作，可以消耗大量的网络资源。因为互联网上网络主机系统分配给一般账户的硬盘容量是有限的，而在这有限的容量中，除了要处理电子邮件外，一般还会用来下载软件或存储个人主页等。用户如果在短时间内收到大量的电子邮件，总容量将超过用户电子邮箱所能承受的负荷。这样，用户的邮箱不仅不能再接收其他人寄来的电子邮件，也会由于"超载"而导致用户端的电子邮件系统功能瘫痪。

有些用户可能会想到利用电子邮件的回复和转发功能还击，将整个炸弹"回复"给发送者。但如果对方将邮件的 From 和 To 都改为用户的电子邮件地址，可想而知这种"回复"的后果是所还击的"炸弹"都会"反弹"回来"炸"自己。如果邮件服务器接收到大量的重复信息和"反弹"信息，邮件总容量迅速膨胀，有可能导致邮件服务器瘫痪。即使是邮件系统还能工作，但也会变得非常迟钝，电子邮件处理的速度会很慢。

3．垃圾邮件

垃圾邮件，顾名思义就是不请自来的、大量散发的、对接收者无用的邮件。垃圾邮件是未经收件者同意，即大量散发的邮件，邮件内容多半以促销商品为目的。它们可能是某些有商业企图的人想利用 Internet 散播广告或色情的媒介。垃圾邮件虽然不像病毒感染一样是一种明显的威胁，但可以很快充满用户的收件箱，使用户难以接收合法的电子邮件。垃圾邮件还是钓鱼者和病毒制造者喜欢的传播媒介。

严格说来，垃圾邮件是一种剽窃行为。传送者只需花极少的代价即可造成收件者的重大损失。假设一个人在每星期收到几十封垃圾邮件，个人用户的损失并非立即显现，但若企业内每个人都收到此类信件时，这对企业网络环境的影响就不仅仅是一件麻烦事了。这些垃圾邮件对企业无任何益处，但是 SMTP 服务器却要承担这些邮件的处理和转发工作。网络资源被这些毫无价值的信件利用来分类、储存和寄发，而那些真正对接收者有用的、含有重大商机的邮件却被淹没在垃圾邮件中。垃圾邮件除了浪费网络资源外，更令人担心的是其附件文件可能夹带病毒，这些病毒将会危害企业网络；附件网址可能附加 Java 或 ActiveX 等恶性程序，许多木马病毒就会借此大量扩散。可以想象，如果让这些未经许可的垃圾邮件继续为所欲为，将造成企业多大的损失。

4．Web 信箱的漏洞

Web 信箱是通过浏览器访问的，部分技术水平不高的站点存在着严重的安全漏洞。比如用户在公共场所(例如网吧)上网浏览自己的邮件时，当关掉当前浏览页面离开后，别人即可利用浏览器做简单操作后就可看到用户刚才浏览过的邮件。如果用户在该机器上注册了新的信箱，其个人资料就会很容易地泄密。

5．网络钓鱼

网络钓鱼(phishing)是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，引诱收信人给出敏感信息的一种攻击方式。攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料(如信用卡号、银行卡账

号、身份证号等内容)。诈骗者通常会将自己伪装成网络银行、在线零售商和信用卡公司等可信的品牌,骗取用户的私人信息。

6. 密码问题

很多人都在强调密码的重要性,然而事实上,很多用户设置的邮箱密码都是很简单、可猜测的。如果要想设置一个好的密码,就要站在一个破解者的角度去思考。破解者最容易想到的是人的生日、用户名、电话号码、信用卡号码、各种执照或证书号码等,虽然这些是人们生活中最容易记住的,但也是最容易被别人猜到的。如果选择的密码在字母中夹杂一些数字和符号,其安全性就要好得多。

7. 监听问题

邮件监听可分为局域网内的监听和来自信箱内部的监听两种方式。一般,使用嗅探器可对局域网内传输的数据进行监听。因为 POP3 协议通常是明文传输,所以很容易就被嗅探器嗅探到邮箱密码。而使用浏览器进行收发邮件就显得相对安全一些。当用户密码被破解之后,攻击者并没有修改密码,而是把信箱设置成转发邮件到攻击者的信箱;然后再在他的信箱中设置转发邮件到这个被破解密码的信箱,同时设置“保留备份”。这样攻击者就可以完全控制该信箱的流量了,因为当他想让用户收邮件时就转发,否则就取消转发,这种方法相当隐蔽。

8. 缓存的危险

用 IE 浏览器在浏览网页时,会在硬盘上开一个临时交换空间,这就是缓存。缓存可能成为攻击者的目标,因为有些信箱使用 Cookie 程序(浏览器中一种用来记录访问者信息的文件)并以明文形式保存密码,同时浏览过的所有网页都存在缓存内,如果缓存被复制,用户的私人信息就不存在秘密了。

9. 冒名顶替

由于普通的电子邮件缺乏安全认证,所以冒充别人发送邮件并不是难事。如果用户不想让别人冒充自己名义发送邮件,可以采用数字证书发送签名/加密邮件(见 4.5.2 小节),这种方式已经被证明是解决邮件安全问题的好办法。

9.2 电子邮件的安全策略和保护措施

用户为保证邮件本身的安全及电子邮件系统的安全性,可采用如下安全策略和保护措施。

1. 防范电子邮件病毒

对电子邮件系统进行病毒防护可从以下几个方面着手。

(1) 思想上要有防病毒意识

首先不要轻易打开陌生人来信中的附件,尤其是一些.exe、.com 类的可执行文件,因为

这些附件极有可能带有计算机病毒或黑客程序，运行后会带来不可预测的后果；其次，对于比较熟悉的朋友发来的电子邮件，如果带有附件却未加说明，最好也不要轻易打开，以防由于朋友的系统感染了病毒而继续传染；第三，不要轻易打开附件中的文件，可先用"另存为"命令将其保存在本地硬盘中，再用查杀病毒软件进行检查，确认无毒后方可打开使用；第四，切忌盲目转发邮件，给别人发送程序文件或电子贺卡时，可先在自己的计算机里试试，确信没有问题后再发出去，以免自己无意中成为病毒的传播者。

（2）使用优秀的防病毒软件进行保护

第一，防病毒软件必须有能力发现并杀灭任何类型的病毒，无论这些病毒是隐藏在邮件文本中，还是躲藏在附件内。当然，有能力扫描压缩文件也是必需的；第二，防病毒软件还必须在收到邮件的同时对该邮件进行病毒扫描，并在每次打开、保存和发送后再进行扫描。

（3）使用防病毒软件同时保护客户机和服务器

一方面，只有客户机的防病毒软件才能访问个人目录，并防止病毒从外部入侵。另一方面，只有服务器的防病毒软件才能进行全局检测和查杀病毒。使用防病毒软件同时保护客户机和服务器是防止病毒在整个系统中扩散的唯一途径，也是阻止病毒入侵没有本地保护但连接到邮件系统的计算机的唯一方法。

2. 防范电子邮件炸弹

平时可采取以下方法防范电子邮件炸弹。

- 使用 Outlook 或 Foxmail 等系统的 POP3 收信工具接收邮件。
- 当你的邮箱被不停地攻击时，先打开一封邮件查看对方地址，然后在收件工具的过滤器中选择不再接收来自该地址的信件，这样就将其直接从电子邮件服务器上删除。
- 接收邮件时，一旦发现邮件列表的数量大大超过平时邮件的数量时，应立即停止下载邮件，然后删除这些邮件炸弹。
- 对邮件地址进行配置，自动删除来自同一主机的过量或重复的消息。

3. 防范垃圾邮件

虽然垃圾邮件可能以任何形式出现，但还是有迹可寻的，它们有以下特点。

- 发信者本身的邮件地址也是假冒的。当用户收到各项难以置信的中奖通知、特价优惠等好消息时需要提高警觉。
- 邮件内容的文法或错字百出。
- 频繁使用大写字体和惊叹语词。
- 大部分的内容为广告或电话服务。

（1）把垃圾邮件放到垃圾邮件活页夹里

如果邮件很多，则需要分类和管理所收到的邮件，清除垃圾邮件是必要的。大多数邮件阅读器都提供垃圾邮件过滤器或一些规则，使用户能清除那些看起来像垃圾的邮件。由于邮件过滤器并不完美，因此不要使用自动清除功能，而应把它们移到垃圾邮件活页夹里不用。偶尔可检查一下这些活页夹，防止丢掉被错当成垃圾的重要邮件。

（2）不随意公开或有意隐藏自己的邮件地址

有许多用户可能不明白，那些垃圾邮件制造者不知道自己的电子邮件地址，怎么能发邮

件给自己呢？其实这并非这些垃圾邮件制造者多么神通广大，而是用户自己在不经意间把自己的地址留在了 Internet 上。那些垃圾邮件制造者使用一种叫 bot 的专用应用程序可搜索 Internet 上的 E-mail 地址。他们的搜索目标可能是各个网址、聊天室、网上讨论区、新闻组、公共讨论区以及其他任何能够充实他们的邮件地址数据库的地方。所以用户避免收到过多垃圾邮件的方法之一就是不随意公开自己的邮件地址。

在实际使用中，有时还避免不了要在一些公共场合中留下自己的邮件地址。为防止非法用户利用这个机会窃取地址信息，可以对自己要公布的邮件地址进行一下“修饰”，使对方能看懂自己的地址而计算机却不能识别。如用户真实的邮件地址是 gongchangzhang@163.com，在电子邮件地址的用户名或主机名前面加上几个字符（如 abc），这样经过修饰后的地址形式就是 gongchangzhang@abc.163.com，然后把该地址填写在邮件编辑窗口的发信人或回复文本栏里。用户可事先与对方约定，比如在正文中加一个注释以提醒对方在回复时要修改地址。这样就把真实的地址隐藏起来了，垃圾邮件制造者自动搜索器搜索到的只能是修饰后的地址而不是原地址。

（3）采用邮件规则过滤功能

在电子邮件中安装过滤器（如 E-mail notify）是一种最有效的防范垃圾邮件的措施。一个优秀的垃圾邮件过滤器能够区分合法邮件和垃圾邮件，并可以使用户的收件箱免受垃圾邮件之苦。在接收任何电子邮件之前预先检查发件人的资料，如果觉得有可疑之处，可以将之删除，不让它进入电子邮件系统，从而保证了邮箱安全。但使用这种组件需要一定的技巧和正确操作，否则就有可能删除掉合法邮件，而保留一些垃圾邮件。但现在的垃圾邮件过滤技术已经很可靠了。

如果你收到一封带有附件的电子邮件，且附件的扩展名为.exe 一类的文件，这时千万不要随意单击运行它，因为这个不明真相的程序很有可能是一个系统破坏程序。攻击者常把系统破坏程序换一个名字用电子邮件发给你，并带有一些欺骗性主题。

因邮件附件中的某些文件可能附带恶意代码，因此在收到带有附件的陌生人的邮件时用户需要格外谨慎。在进行规则设置时应予以考虑。在防范邮件附件可能带有恶意代码时，用户应采取如下基本策略。

① 除非自己确实需要某个附件，否则不要下载或打开它。

② 在确信邮件附件的安全性之前不要打开它。

③ 在打开一个附件中的可执行文件前需要保持高度的警惕。

4. 电子邮件加密和签名

Internet 是一个包含了成千上万服务器、路由器和中继器的大型网络，用户所发送的电子邮件在到达目的地之前需要经过若干个地方。在任意一个地方，只要懂得一些访问以及网络知识的人都知道如何来阅读电子邮件。从技术上看，没有任何方法能够阻止攻击者截取电子邮件数据包，用户无法确定自己的邮件将会经过哪些路由器，也不能确定经过这些路由器时会发生什么。

从邮件本身安全的角度看，既要保证邮件不被无关的人窃取或更改，又要使接收者能确定该邮件是由合法发送者发出的。可以对邮件使用加密和数字签名技术来达到这个目的。经过加密和数字签名处理后的邮件，即使攻击者得到邮件数据包后也无法阅读它。作为

Internet 标准而提出的增强型加密邮件 PEM 和 PGP 软件是实现文件和邮件加密的两个具有代表性的加密软件。邮件加密可以保护用户的秘密，确保邮件不能被无关人员阅读，除非有人知道用户的密码以及解密的口令。

如果用户的 E-mail 软件中设置了加密的功能，就可以通过单击某个按钮的操作来加密用户的邮件。那么就只有合法收件人能够阅读信件，他必须有一个相匹配的密钥和正确的口令。对于其他人来说这封信可能是空的，也可能是乱码。

对于邮件加密，需要考虑采用什么样的加密方法。对称密码算法加密简便高效，也较安全，但其密钥管理十分困难；公钥密码算法加密密钥管理方便，也便于数字签名，但加密解密速度慢，效率低。所以在实际使用中将两者结合起来，充分发挥各自的优势。

5. 谨慎使用自动回信功能

所谓自动回信就是指当对方发来一封邮件而你没有及时收取时，邮件系统会按照你事先的设定自动给发信人回复一封确认收到该邮件的回信。该功能本来可给用户带来方便，但也有可能形成邮件炸弹。试想，如果对方使用的邮件系统也开启了自动回信功能，那么当收到你自动回复确认信时，恰巧他也没有及时收取信件，他的系统就会自动给你发送一封确认收到邮件的回信。这样，这种自动回复的确认信便会在双方的邮件系统中不断重复发送，直到形成邮件炸弹使双方的邮箱都爆满为止。因此一定要慎重使用自动回信功能。

6. 保护邮件列表中的 E-mail 地址

如果用户与许多人通过 E-mail 就某个主题进行讨论，从而要把 E-mail 地址列入公共邮件地址清单中。这种讨论组类似于新闻组，只不过它是通过 E-mail 进行的。这些公共讨论经常加载在网上，这对于垃圾邮件制造者来说是很有吸引力的。把 E-mail 地址列入单向邮件列表或通过有良好信誉的地方登记到邮件公告板上，可避免使用户的地址列入垃圾邮件制造者的名单。好的邮件公告板组织的软件会有严格的保护措施来防止外来者获取注册者地址。

7. 使用安全的邮件客户端

客户端系统是用户用来编写、发送和接收电子邮件的软件。保障电子邮件系统安全的基本要求就是采用一个安全的邮件客户端系统。有些邮件客户端的漏洞较多，而厂商的补丁又很滞后，这就为黑客攻击提供了方便。

9.3　电子邮件的安全设置实例

针对电子邮件的安全问题，用户可有目的地增加邮件规则和进行系统安全方面的设置。一般不同的邮件服务商会提供不同的 Web 管理方式，通过 Web 进入自己的邮箱（如 Hotmail 邮箱、Yahoo 邮箱等），可以在邮件系统的帮助下进行邮件的安全设置。另外，Outlook Express 和 Foxmail 等专用的邮件收发和管理工具对电子邮件的安全有更方便的地方。

1．浏览器的安全设置

浏览器种类很多，这里以 IE 浏览器为例。进入 IE 浏览器，选择“工具”→“Internet 属性”菜单，进入“安全”选项卡，在这里可以对四种不同区域（Internet、本地 Intranet、受信任的站点和受限制的站点）分别进行安全设置，如图 9.1 所示。选择 Internet 区域单击“自定义级别”按钮，弹出如图 9.2 所示的窗口。在此窗口用户可按照自己的安全考虑选择相关组件和设定安全级别。



图 9.1　浏览器 Internet 选项



图 9.2　Internet 自定义安全设置

在如图 9.1 所示的“隐私”选项卡中进行设置可以适当保护用户自己的隐私。如果担心信件内容的泄露，可以在图 9.1 所示的“内容”选项卡中进行证书设置。

2．邮件规则的设置

下面以微软的 Outlook Express 为例介绍邮件规则的安全设置。打开 Outlook Express，依次选择“工具”→“邮件规则”→“邮件”菜单，弹出“新建邮件规则”窗口，如图 9.3 所示。如果在“选择规则条件”栏勾选后，再在“选择规则操作”栏勾选需要的操作，然后在“规则描述”中就自动出现了新建的邮件规则说明。如在“选择规则条件”栏勾选“若邮件带有附件”选项，在“选择规则操作”栏勾选“移动到指定的文件夹和将邮件标记为忽略”两项，则在“规则描述”中就出现“邮件带有附件移动到指定的文件夹和将邮件标记为被监测”选项；如在“选择规则条件”栏勾选“若邮件长度大于指定的大小”选项，在“选择规则操作”栏勾选“删除”，在“规则描述”中就出现“若邮件长度大于指定的大小删除”选项，如图 9.4 所示。

当用户连续收到很多不熟悉的发件人的邮件，特别是多次收到一个地址的邮件或带有很大附件的邮件时，就要考虑这些可能是垃圾邮件了，这就可以通过设置过滤规则对垃圾邮件进行限制。打开 Outlook Express，依次选择“工具”→“邮件规则”→“阻止发件人名单”菜单，在弹出的“邮件规则”窗口中单击“添加”按钮，输入你想阻止的电子邮件地址（如 abcd@163.com），确定后显示在窗口中，如图 9.5 所示。还可以继续添加其他的想要



图 9.3　新规则设置(1)



图 9.4　新规则设置(2)

阻止的发送人地址。这样，你就不会再收到这些被阻止的邮件地址发来的邮件了。

3. 使用纯文本格式

HTML 格式的文档可能含有在未得到用户许可情况下就能够执行某些操作的因素。在用户单击时，它就可能将用户带到一个陌生的网站。虽然多数客户端软件可以起到保护作用，但用户最好禁用 HTML 格式，而采用纯文本格式。

Outlook Express 下使用纯文本的方法：打开 Outlook Express，选择“工具”→“选项”菜单，单击“阅读”选项卡，选中“用纯文本格式阅读所有信息”项并单击“确定”按钮即可，如图 9.6 所示。



图 9.5 “阻止发件人”设置

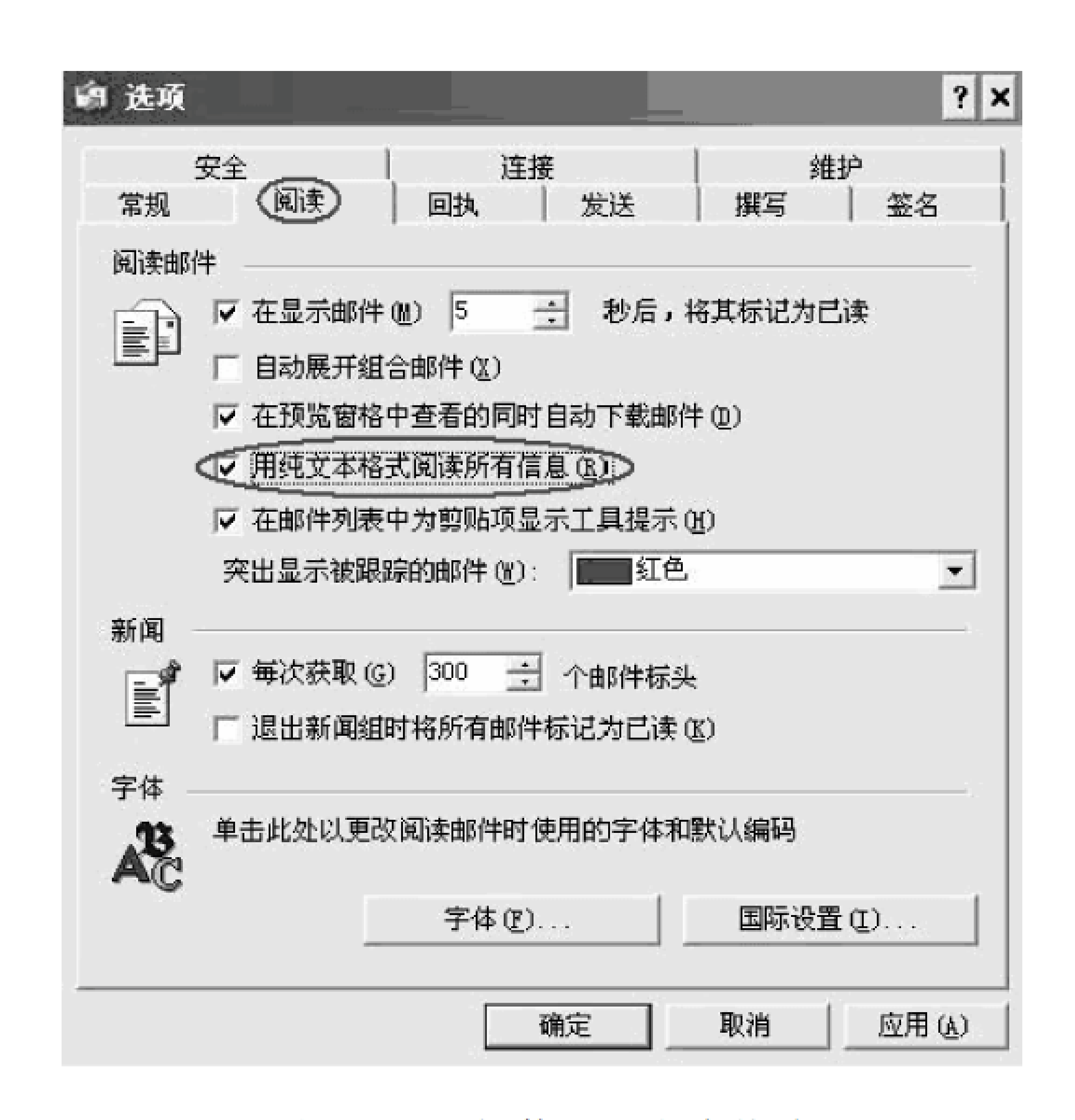


图 9.6 选择使用纯文本格式

4. 使用多层防御

就像对付恶意软件一样，要保护邮件系统的安全，需要采用多种防御措施，使这些措施能有效地对付网络威胁。

(1) 客户端的安全设置

事实上，所有主要的邮件客户端都提供安全设置特性、反垃圾邮件、防钓鱼等功能。用户可通过这些功能阻止相关的威胁。

(2) 使用防火墙

许多企业级防火墙不但可以阻止网络攻击，还可以通过过滤附件中的恶意代码来保障

邮件系统的安全性。当然这需要预先在防火墙中设置相关的规则。

(3) 加密邮件

保护电子邮件安全不但要防止恶意邮件到达用户桌面,还要保护发出邮件的安全和保密。采用加密措施,即可将发送的邮件变为一种非授权人员无法阅读的形式,从而保护电子邮件的机密性。在发送电子邮件过程中,用户还可以采用加密的传输通道。如在 Outlook Express 中,选择"工具"→"选项"菜单,单击"安全"选项卡,如图 9.7 所示。在这里用户除了勾选相应的项目外,还应进行"数字标识"(证书)和"获取数字标识"等设置。

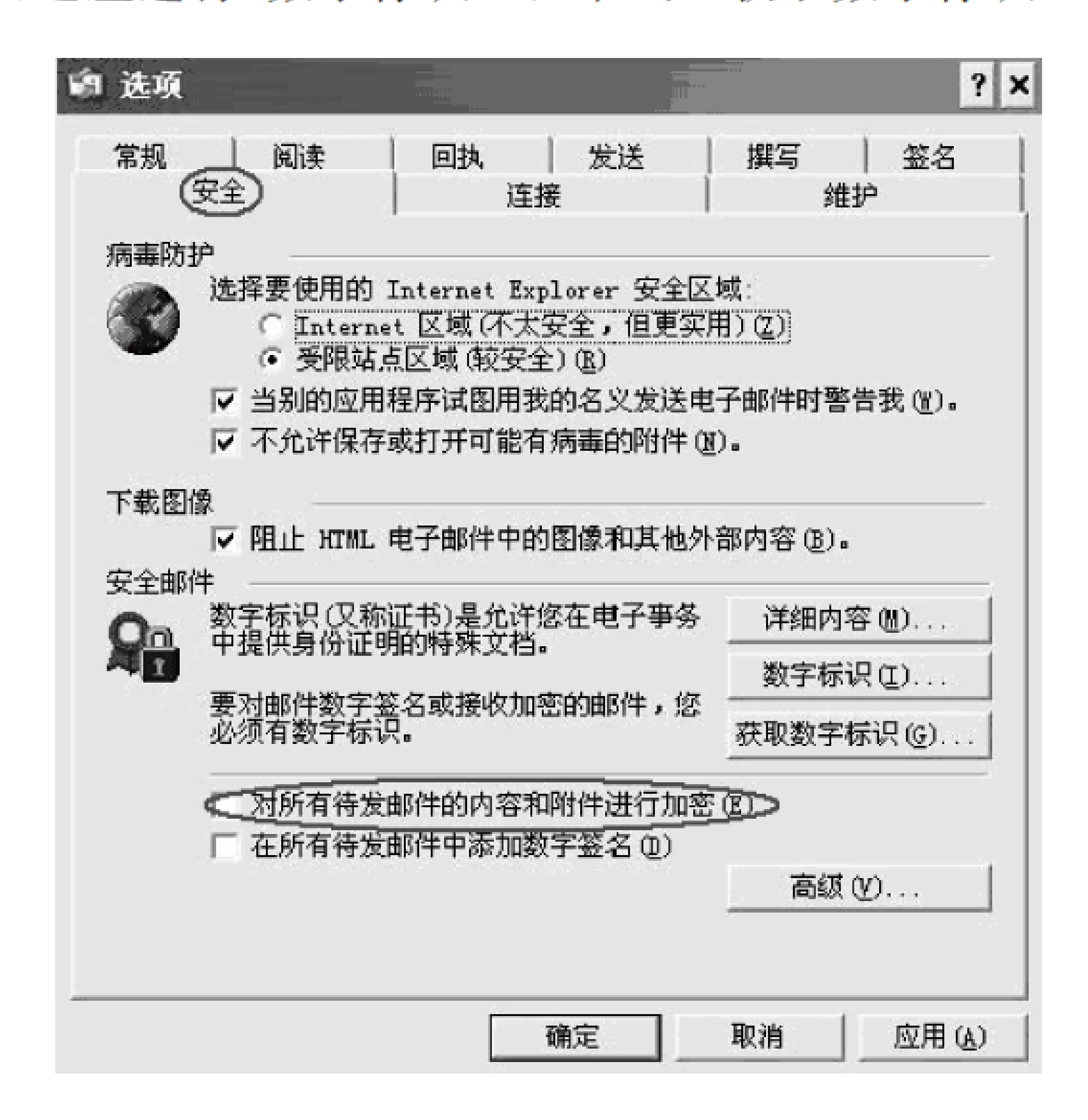


图 9.7 Outlook 的邮件加密设置

(4) 运用反病毒工具

目前,许多反病毒工具都可以嵌入到 Outlook Express 等邮件客户端,并可以查找和清除邮件中的病毒、蠕虫和特洛伊木马等。如图 9.8 所示的 NOD32 软件就具有病毒防护和 Web 保护等功能。

5. 备份邮件资料

与系统和服务器一样,Outlook Express 也可以对重要的资料进行备份,以防在资料丢失或当资料被破坏时可以及时恢复。默认情况下,Outlook Express 邮件的保存位置是 C:WINDOWS\...\ApplicationData\Identities{4C0ABEE0-5D39-11D6-B814-9E1F7480B676}\Microsoft\OutlookExpress 文件夹,其中{}中的符号不是固定的,它与不同用户的计算机环境有关。将该文件夹中的所有文件复制到 E:mymail,操作步骤为:在 Outlook Express 中选择"工具"→"选项"菜单,单击"维护"选项卡,再单击"存储文件夹"按钮,在弹出的"存储位置"窗口中单击"更改"按钮,指定存储位置为 E:mymail 文件夹,最后单击"确定"按钮即可,如图 9.9 所示。同样,可以对通讯簿进行转移,Outlook Express 的通讯簿文件保存在 C:WINDOWS\...\ApplicationData\Microsoft\Address Book 文件夹中,将这个文件夹中的.wab 文件复制到其他文件夹中(如 E:mytx)注册表编辑器,依次找到 HKEY_CURRENT_

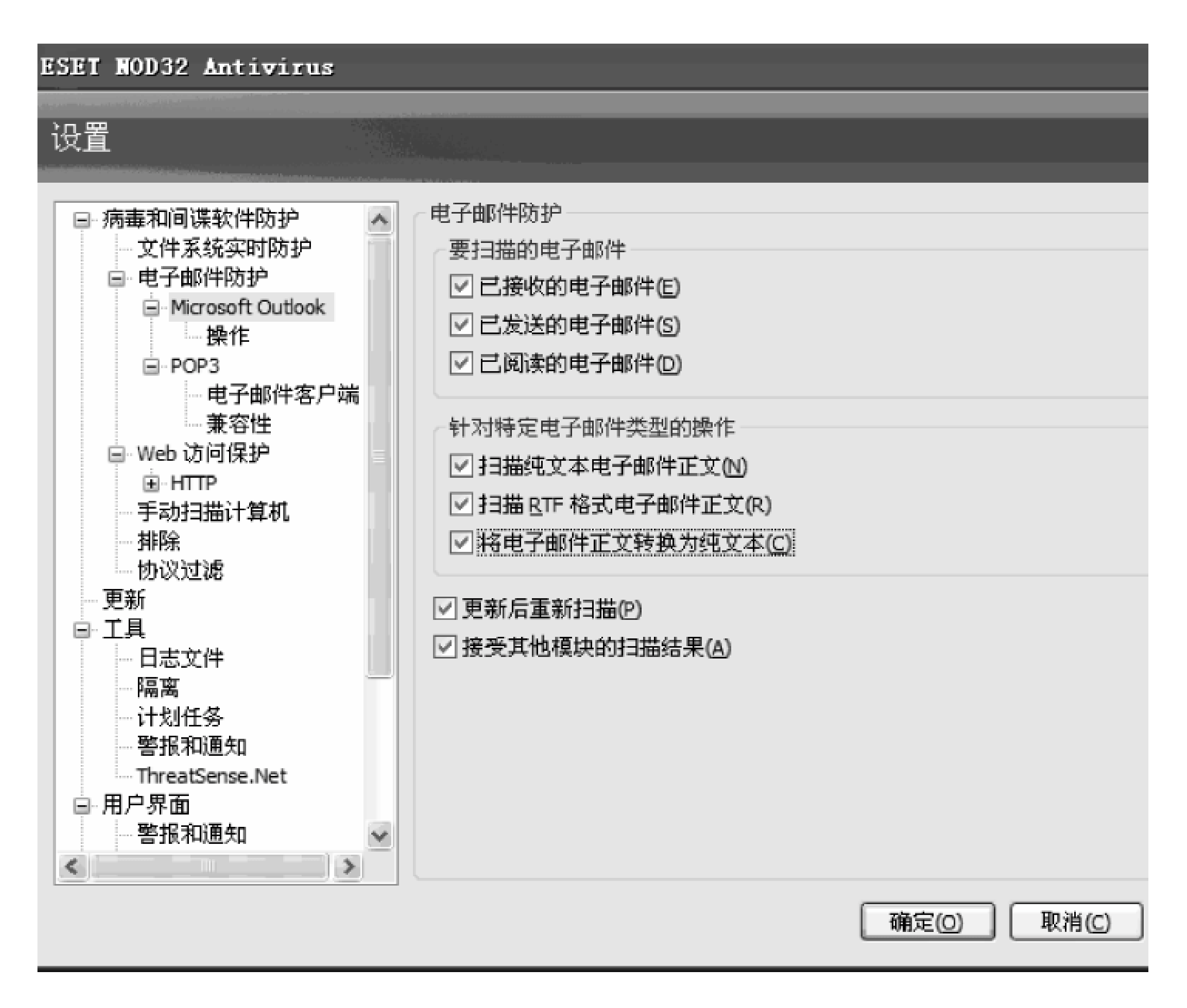


图 9.8　NOD32 的病毒防护和 Web 保护功能

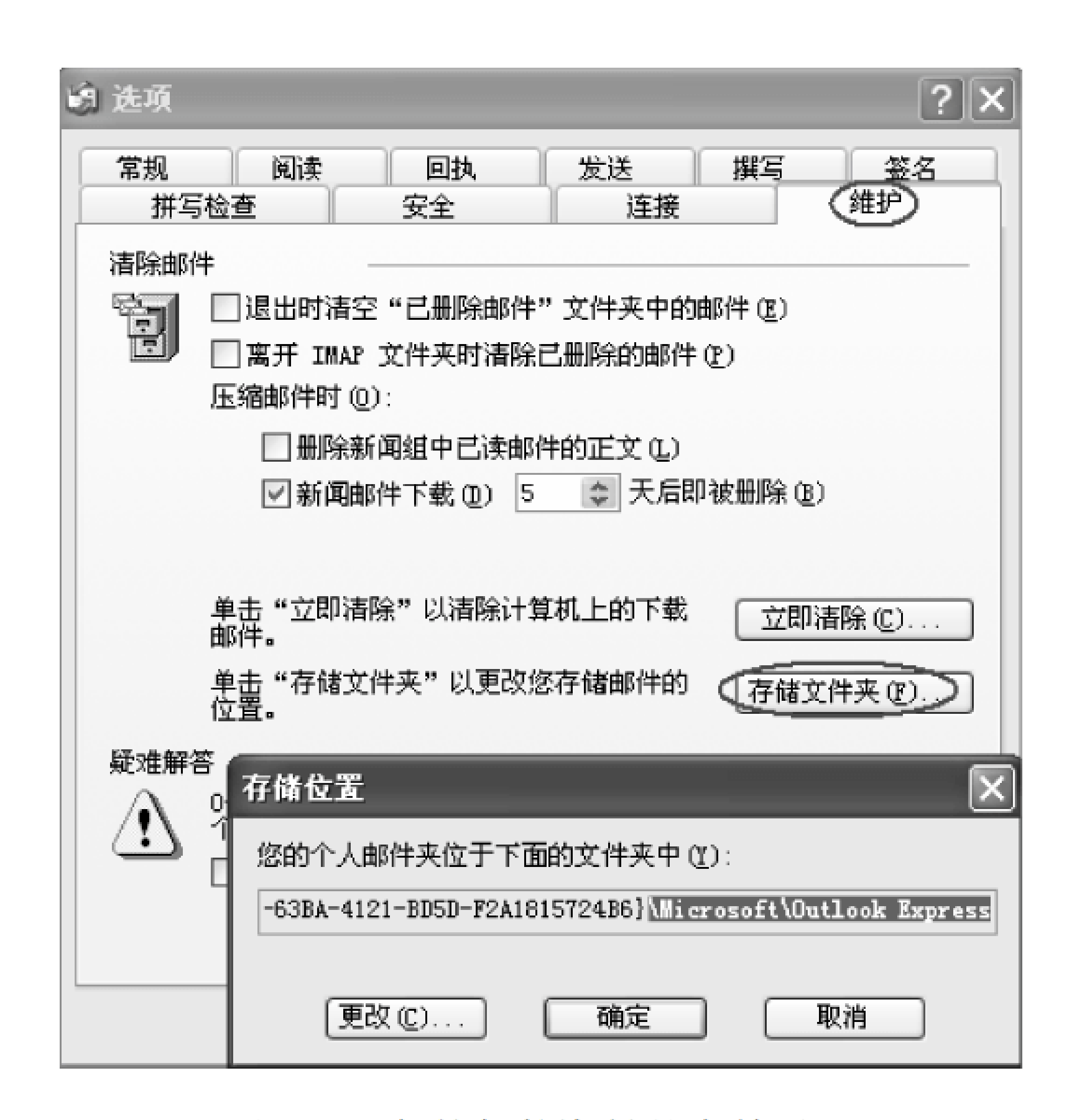


图 9.9　备份邮件资料的存储设置

USERSoftwareMicrosoftWABWAB4WabFileName 子键分支，然后将其默认值更改为自己的文件夹 E:mytx 即可。

6. 拒绝 Cookie 信息

许多网站会使用一些不易被察觉的技术，暗中搜集你填写在表格中的电子邮件信息，最

常见的就是利用Cookie程序记录访客上网的浏览行为和习惯。如果你不想让Cookie程序记录你的个人隐私信息,则可以在浏览器中做一些必要的设置,要求浏览器在接受Cookie之前提醒你,或者干脆拒绝它们。随着时间的推移,Cookie程序记录信息可能越来越多。为了确保安全,应将这些已有的Cookie信息从硬盘中清除掉,并在浏览器中调整Cookie设置,让浏览器拒绝接受Cookie信息。屏蔽Cookie的操作步骤为:在图9.1所示"安全"选项卡下单击"自定义级别"按钮;在打开的图9.2所示的"安全设置"对话框中找到关于Cookie的设置,然后选择"禁用"或"提示"选项即可。

如果在公共场所收发信件,保护信件内容的隐私性是很重要的。可以通过"Internet选项"的"常规"选项卡设置,如图9.10所示。单击删除文件、清除历史记录以及删除Cookie即可清除一些隐私信息。另外,还可以到如图9.11所示的"内容"选项卡的"个人信息"栏进行单击"自动完成"按钮自动完成设置,清除表单及密码等。

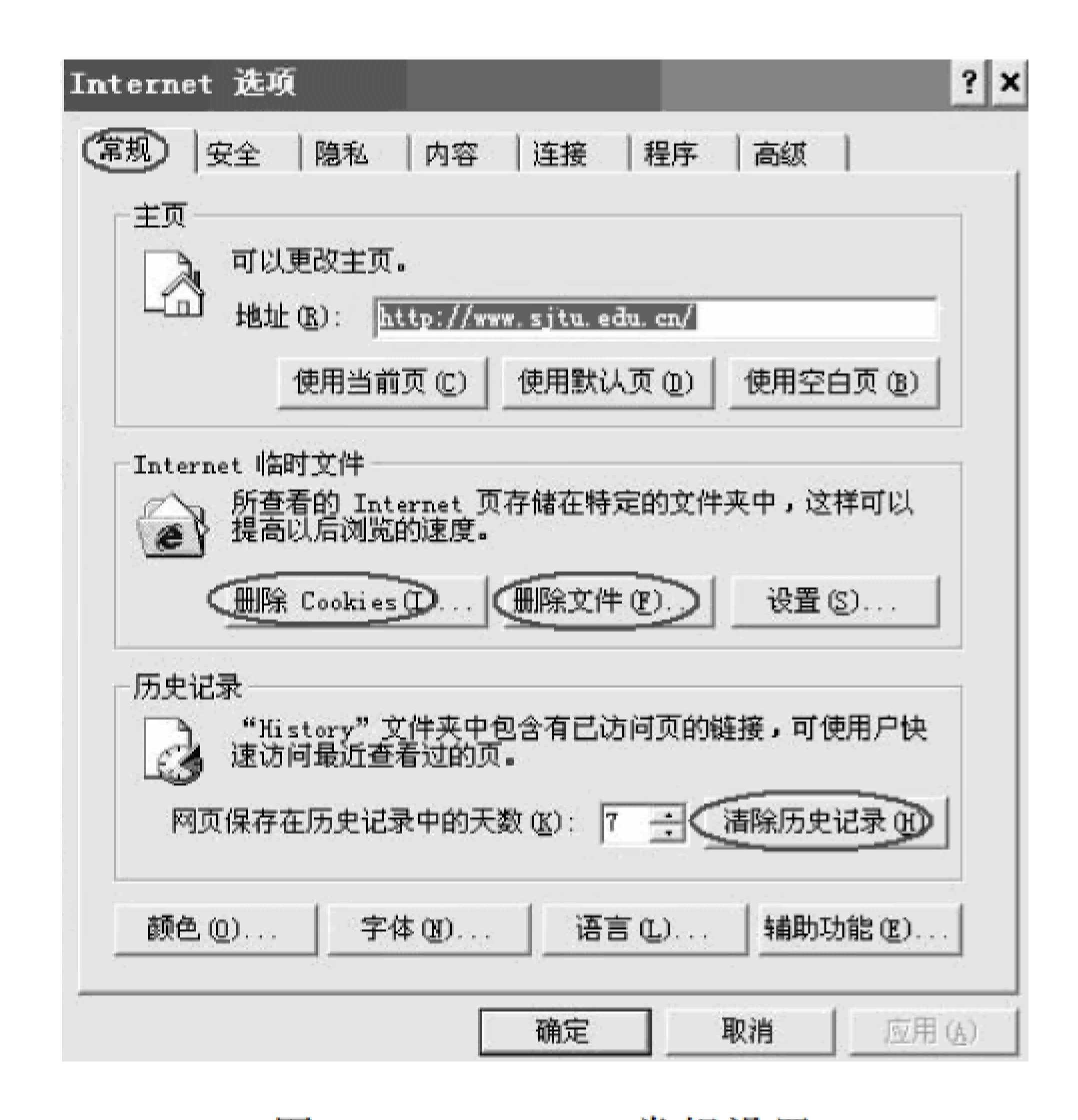


图9.10 Internet常规设置

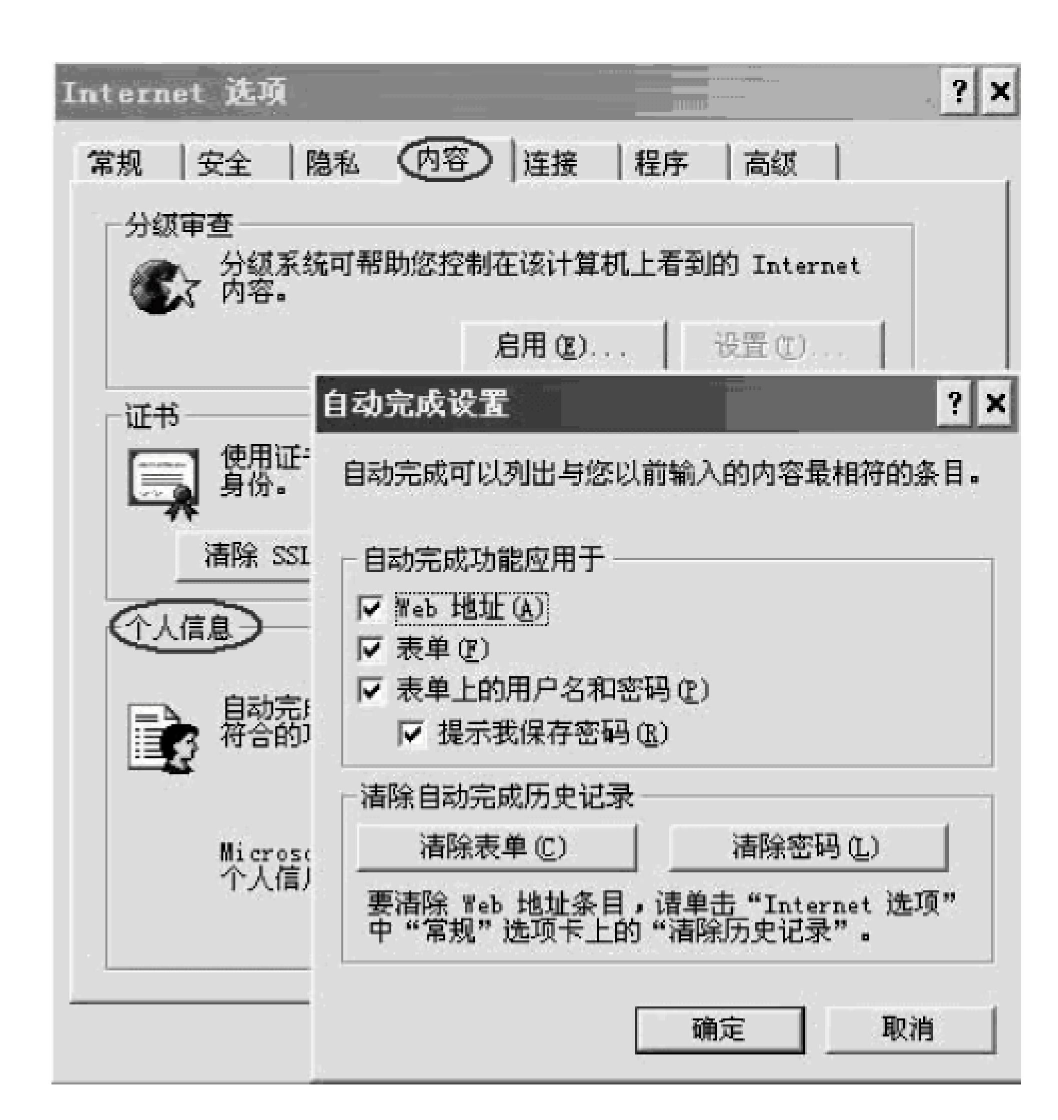


图9.11 清除隐私的自动设置

习题和思考题

一、问答题

1. 什么是垃圾邮件?如何防范垃圾邮件?
2. 如何防范电子邮件病毒?
3. 简述电子邮件的安全漏洞。
4. 简述几种保护电子邮件安全的措施。

二、填空题

1. 实现邮件加密的两个代表性的软件是(　　)和(　　)。
2. 电子邮件病毒的传播速度(　　),传播范围(　　),绝大多数电子邮件病毒都有(　　)能力。

三、单项选择题

1. 以下(　　)项电子邮件威胁属于垃圾邮件。

A. 邮件病毒　　B. 邮件密码不安全　　C. 网络钓鱼　　D. 冒名顶替

2. 以下(　　)项措施可预防垃圾邮件。

A. 加密邮件　　B. 隐藏自己的邮件地址

C. 采用纯文本格式　　D. 拒绝 Cookie 信息

四、实验题

1. 以 Outlook Express 为例,对邮件规则过滤功能进行设置,采取措施防范垃圾邮件,对电子邮件进行加密和签名。

2. 以 Foxmail 为例,进行邮件的安全设置和应用。

附录A 部分习题答案

第1章

二、填空题

1. 可靠性
2. 可用性
3. 被动　主动
4. 自然环境　网络中信息
5. 信息内容或信息的长度、传输频率等特征
6. 故意
7. 无意
8. 主动
9. 全盘恢复　个别文件恢复

三、单项选择题

1. A　2. B　3. C　4. B　5. D　6. C　7. A　8. (1) B (2) A
9. (1) A (2) C (3) B (4) D (5) A

第2章

二、填空题

1. 主机、显示器、打印机等　Hub、交换机、路由器、网络线缆、各种服务器等
2. 增加一些多余设备
3. 核心交换机　服务器　存储设备
4. 路由器
5. 静态　动态
6. 交换机
7. 安全认证　防火墙
8. 文件服务器　数据库服务器　通信服务器

第3章

二、填空题

1. 自主访问控制　强制访问控制

2. 自主访问控制
3. 数字证书验证　生理特征验证
4. 存储器保护　访问控制　身份认证
5. 用户账户和口令　账户锁定　安全标识符
6. 对于大型软件系统在使用过程中暴露的问题而发布的解决问题的小程序
7. 自动更新

三、单项选择题

1. (1) D　(2) C　(3) D
2. A

第 4 章

二、填空题

1. 加密　密文　明文
2. DES　IDEA　3DES
3. RSA　背包算法　ElGamal　复杂的数学难题
4. 密钥的保密强度
5. 对称　128　64
6. 密码编码学　密码分析学　密码编码学　编码技术　被保护信息　指定接收者　密码分析学　攻破一个密码系统　本来面目　前者　后者
7. 识别　在访问者声明自己的身份后系统要对他所申明的身份进行验证　秘密
8. 是相同的
9. 算法容易实现、速度快
10. IEDA　RSA　加密　签名　IDEA　RSA　邮件加密　数字签名
11. RSA　DSS/DSA　Hash
12. 不可否认
13. 数据加密标准(DES)　公钥密码体制　密码学

三、单项选择题

1. B　2. A　3. C　4. A　5. C　6. A　7. A　8. D　9. B　10. D

第 5 章

二、填空题

1. IP　TCP
2. 无连接的　不可靠的　尽最大努力的
3. 身份验证　保密性
4. 主机对主机　IP
5. 进程对进程
6. 修改和扩充
7. SET　PEM
8. 文件加密工具　公共密钥加密　文件加密

9. 加密　自动解密
10. Windows 2000/XP/2003 操作系统　NTFS 分区格式
11. 网络认证服务　对称密钥密码体制　保密性和完整性
12. 加密和认证　窃听和篡改　网络攻击
13. 网络认证协议 AH　封装安全载荷协议 ESP　密钥管理协议 IKE
14. IPv6　隧道模式　传输模式
15. 加密和验证　对数据包包头进行完整性验证　对数据的加密和完整性验证

三、单项选择题

1. D　2. D　3. C　4. C

第 6 章

二、填空题

1. 传播速度快　清除难度大
2. 管理　技术
3. 包过滤　服务代理　状态检测
4. 终端客户　Internet
5. 拒绝服务　利用　信息收集
6. 缓冲区溢出
7. 拒绝服务
8. 被动　主动
9. 硬件故障　网络线路威胁　电磁辐射
10. 应用软件漏洞　操作系统漏洞　通信协议漏洞

三、单项选择题

1. C　2. B　3. A　4. D　5. D　6. C　7. B　8. (1) B　(2) D　(3) A
9. (1) A　(2) D　10. (1) C　(2) D

第 7 章

二、填空题

1. 认证　访问控制　数据的保密性
2. 隧道　加密/解密　密钥管理　身份认证
3. 路由器　防火墙

三、单项选择题

1. D　2. C

第 8 章

二、填空题

1. MMDS　LMDS　扩频
2. 数据加密
3. 900　1800

4. 加密
5. TKIP　AES　IEEE 802.1x

三、单项选择题

1. (1) D　(2) B　(3) B　(4) C
2. C

第 9 章

二、填空题

1. PEM　PGP
2. 快　广　自我复制

三、单项选择题

1. C　2. B

参 考 文 献

1. 阙喜戎.信息安全原理及应用.北京：清华大学出版社，2009.
2. 黄传河.网络安全防御技术实践教程.北京：清华大学出版社，2009.
3. 邓吉.黑客攻防实战编程.北京：电子工业出版社，2009.
4. 田园.网络安全教程.北京：人民邮电出版社，2009.
5. 刘晓辉.网络安全设计、配置与管理大全.北京：电子工业出版社，2009.
6. 韦文思.信息安全防御技术与实施.北京：电子工业出版社，2009.
7. 胡道元.网络安全.2版.北京：清华大学出版社，2008.
8. 王群.计算机网络安全技术.北京：清华大学出版社，2008.
9. 石淑华.计算机网络安全技术.2版.北京：人民邮电出版社，2008.
10. 石志国.计算机网络安全教程.北京：清华大学出版社，2007.
11. 张敏波.网络安全实战详解.北京：电子工业出版社，2008.
12. 张京生.数据恢复方法及案例分析.北京：电子工业出版社，2008.
13. 林涛.计算机网络安全技术.北京：人民邮电出版社，2007.
14. 徐茂智.信息安全与密码学.北京：清华大学出版社，2007.
15. 赵安军.网络安全技术与应用.北京：人民邮电出版社，2007.
16. 张庆华.网络安全与黑客攻防宝典.北京：电子工业出版社，2007.
17. 胡昌振.网络入侵检测原理与技术.北京：北京理工大学出版社，2006.
18. 张友纯.计算机网络安全.武汉：华中科技大学出版社，2006.
19. 邵波.计算机网络安全技术及应用.北京：电子工业出版社，2005.
20. 梁亚声等.计算机网络安全技术教程.北京：机械工业出版社，2004.
21. http://www.110ok.cn/(中国安防技术网).2010年1月15日.
22. http://forum.chinesehonker.org/(中国红客联盟).2010年1月15日.
23. http://www.chinawill.com(中国鹰派联盟).2010年1月15日.
24. http://www.redhacker.cn/(中国红盟).2010年1月15日.
25. http://www.isccc.gov.cn/(中国信息安全认证中心).2010年1月15日.
26. http://www.cnpaf.net/forum/forumdisplay.php?fid=4&filter=type&typeid=6&sid=vXGX4b(中国协议分析网).2010年1月15日.
27. http://tech.ccidnet.com/col/1101/1101.html(赛迪网IT安全技术).2010年1月15日.
28. http://www.nsfocus.net(中联绿盟信息技术有限公司技术版).2010年1月15日.
29. http://www.duba.net(金山毒霸).2010年1月15日.
30. http://www.jiangmin.com(北京江民科技有限公司).2010年1月15日.
31. http://www.pgpi.org(国际PGP网站).2010年1月15日.
32. http://bbs.hackbase.com/forumdisplay.php?fid=128&page=2(系统攻防技术黑基论坛).
33. http://www.360.cn(360安全卫士官方网站).2010年1月15日.
34. http://www.cnpaf.net/forum/forumdisplay.php?fid=4&filter=type&typeid=6&sid=vXGX4b(中国协议分析网之网络安全论坛).2010年1月15日.
35. http://network.51cto.com/(51CTO-IT技术网站).2010年1月15日.
36. http://blog.ixpub.net/(IXPUB技术博客).2010年1月15日.
37. 软考资讯网. 交换机网络安全策略全方位解析. http://www.softexam.cn/eschool/details.asp?id=

12367. 2010 年 1 月 15 日.
38. Linux下的(VRRP)虚拟路由冗余协议介绍. http://www. yuanma. org/data/2006/0629/article_1022. htm. 2010 年 1 月 15 日.
39. 设置好 NAT 地址转换 网络安全更有保障. http://zl. pcw. com. cn/post/109/44964. 2010 年 1 月 15 日.
40. TCP/IP的安全性. http://www. cnpaf. net/forum/viewthread. php? tid=113. 2010 年 1 月 15 日.
41. [基础课程]之 EFS 加密和安全. http://bbs. zdnet. com. cn/viewthread. php? tid=17742. 2010 年 1 月 15 日.
42. 重要文件的铠甲：EFS 加密. http://www. pconline. com. cn/pcjob/system/microsoft/article/0408/444298. html. 2010 年 1 月 15 日.
43. kerberos的安装配置. http://it. china-b. com/lirm/445419. html. 2010 年 1 月 15 日.
44. IPSec技术合集. http://www. ixpub. net/viewthread. php? tid=772362&extra=&page=1. 2010 年 1 月 15 日.
45. 关振胜. IPSec. http://book. 51cto. com/art/200807/82236. htm. 2010 年 1 月 15 日.
46. 平时上网需不需要设防火墙呢. http://zhidao. baidu. com/question/36380844. html. 2010 年 1 月 15 日.
47. http://bbs. kafan. cn(卡饭网——计算机完全交流中心). 2010 年 1 月 15 日.
48. 路由器精确控制访问. http://www2. ccw. com. cn/1999/40/180374. shtml. 2010 年 1 月 15 日.
49. 系统安全之用 Windows 自带功能保护秘密. http://chapi. blogbus. com/logs/2007/1/. 2010 年 1 月 15 日.
50. 专题教程之 VPN 技术专题. http://www4. it168. com/jtzt/shenlan/zhuanti/vpn/. 2010 年 1 月 15 日.
51. TL-WR340G+ 54M无线宽带路由器二级路由设置方法(原创). http://www. 52mis. com. cn/post/105. html. 2010 年 1 月 15 日.
52. 新浪科技. Foxmail 5 安全电子邮件功能应用初接触(2). http://tech. sina. com. cn/c/2003-08-31/22421. html. 2010 年 1 月 15 日.